ON THE FIELD INTERSECTION PROBLEM OF SOLVABLE QUINTIC GENERIC POLYNOMIALS

AKINARI HOSHI AND KATSUYA MIYAKE

ABSTRACT. We study a general method of the field intersection problem of generic polynomials over an arbitrary field k via formal Tschirnhausen transformation. In the case of solvable quintic, we give an explicit answer to the problem by using multi-resolvent polynomials.

1. INTRODUCTION

Let G be a finite group. Let k be an arbitrary field and $k(\mathbf{t})$ the rational function field over k with n indeterminates $\mathbf{t} = (t_1, \ldots, t_n)$.

A polynomial $f_{\mathbf{t}}(X) \in k(\mathbf{t})[X]$ is called k-generic for G if it has the following property: the Galois group of $f_{\mathbf{t}}(X)$ over $k(\mathbf{t})$ is isomorphic to G and every G-Galois extension $L/M, \#M = \infty, M \supset k$, can be obtained as $L = \mathrm{Spl}_M f_{\mathbf{a}}(X)$, the splitting field of $f_{\mathbf{a}}(X)$ over M, for some $\mathbf{a} = (a_1, \ldots, a_n) \in M^n$. We suppose that the base field M, $M \supset k$, of a G-extension L/M is an infinite field.

Examples of k-generic polynomials for G are known for various pairs of (k, G) (for example, see [Kem94], [KM00], [JLY02], [Rik04]). Let $f_{\mathbf{t}}^G(X) \in k(\mathbf{t})[X]$ be a k-generic polynomial for G. Since a k-generic polynomial $f_{\mathbf{t}}^G(X)$ for G covers all G-Galois extensions over $M \supset k$ by specializing parameters, it is natural to ask the following problem:

Field isomorphism problem of a generic polynomial. Determine whether $\mathrm{Spl}_M f_{\mathbf{a}}^G(X)$ and $\mathrm{Spl}_M f_{\mathbf{b}}^G(X)$ are isomorphic over M or not for $\mathbf{a}, \mathbf{b} \in M^n$.

It would be desired to give an answer to the problem within the base field M by using the data $\mathbf{a}, \mathbf{b} \in M^n$. Let S_n (resp. D_n, C_n) be the symmetric (resp. the dihedral, the cyclic) group of degree n. For C_3, the polynomial $f_t^{C_3}(X) = X^3 - tX^2 - (t+3)X - 1 \in k(t)[X]$ is k-generic for an arbitrary field k. We showed in [HM] the following theorem which is an analogue to the results of Morton [Mor94] and Chapman [Cha96].

Theorem 1.1 ([Mor94], [Cha96], [HM]). *Let $f_t^{C_3}(X)$ be as above and assume char $k \neq 2$. For $m, n \in M$ with $(m^2 + 3m + 9)(n^2 + 3n + 9) \neq 0$, two splitting fields $\mathrm{Spl}_M f_m^{C_3}(X)$ and $\mathrm{Spl}_M f_n^{C_3}(X)$ over M coincide if and only if there exists $z \in M$ such that either*

$$n = \frac{m(z^3 - 3z - 1) - 9z(z+1)}{mz(z+1) + z^3 + 3z^2 - 1} \text{ or } n = -\frac{m(z^3 + 3z^2 - 1) + 3(z^3 - 3z - 1)}{mz(z+1) + z^3 + 3z^2 - 1}.$$

We have $\mathrm{Spl}_M f_m^{C_3}(X) = \mathrm{Spl}_M f_n^{C_3}(X)$ whenever $m, n \in M$ satisfy the condition in Theorem 1.1. In particular, over an infinite field M, for each fixed $m \in M$ with $\mathrm{Gal}(f_m^{C_3}/M) = \{1\}$ or $\mathrm{Gal}(f_m^{C_3}/M) = C_3$ there exist infinitely many $n \in M$ such that $\mathrm{Spl}_M f_m^{C_3}(X) = \mathrm{Spl}_M f_n^{C_3}(X)$.

We also gave analogues to Theorem 1.1 for two non-abelian groups for S_3 and D_4 in [HM07] and [HM-2] respectively as follows:

2000 *Mathematics Subject Classification.* Primary 11R16, 11R20, 12F10, 12F12.

Key words and phrases. Generic polynomial, field isomorphism problem, subfield problem, field intersection problem, formal Tschirnhausen transformation.

This work was partially supported by Grant-in-Aid for Scientific Research (C) 19540057 of Japan Society for the Promotion of Science.

Theorem 1.2 ([HM07])**.** *Let k be a field of char $k \neq 3$ and $f_t^{S_3}(X) = X^3 + tX + t \in k(t)[X]$ a k-generic polynomial for S_3. For $a, b \in M \setminus \{0, -27/4\}$ with $a \neq b$, two splitting fields $\mathrm{Spl}_M f_a^{S_3}(X)$ and $\mathrm{Spl}_M f_b^{S_3}(X)$ over M coincide if and only if there exists $u \in M$ such that*

$$b = \frac{a(u^2 + 9u - 3a)^3}{(u^3 - 2au^2 - 9au - 2a^2 - 27a)^2}.$$

Theorem 1.3 ([HM-2])**.** *Let k be a field of char $k \neq 2$ and $f_{s,t}^{D_4}(X) = X^4 + sX^2 + t \in k(s,t)[X]$ a k-generic polynomial for D_4. For $a, b \in M$, we assume that $\mathrm{Gal}(f_{a,b}^{D_4}/M) = D_4$. Then for $a, b, a', b' \in M$, two splitting fields $\mathrm{Spl}_M f_{a,b}^{D_4}(X)$ and $\mathrm{Spl}_M f_{a',b'}^{D_4}(X)$ over M coincide if and only if there exist $p, q \in M$ such that either*

$$\text{(i)} \quad a' = ap^2 - 4bpq + abq^2, \quad b' = b(p^2 - apq + bq^2)^2 \quad \text{or}$$
$$\text{(ii)} \quad a' = 2(ap^2 - 4bpq + abq^2), \quad b' = (a^2 - 4b)(p^2 - bq^2)^2.$$

In Theorem 1.3, under the assumption $C_4 \leq \mathrm{Gal}(f_{a,b}^{D_4}/M) \leq D_4$, there exist $p, q \in M$ which satisfy the condition (i) if and only if $M[X]/(f_{a,b}^{D_4}(X)) \cong_M M[X]/(f_{a',b'}^{D_4}(X))$ (cf. [HM-2, Lemma 4.14]), and this fact was given by Van der Ploeg [Plo87] when $M = \mathbb{Q}$.

As in the case of C_3 over an infinite field M, for a fixed $a \in M$ with $\mathrm{Gal}(f_a^{S_3}/M) \leq S_3$ (resp. fixed $a, b \in K$ with $C_4 \leq \mathrm{Gal}(f_{a,b}^{D_4}/M) \leq D_4$) there exist infinitely many $b \in M$ (resp. $a', b' \in M$) such that $\mathrm{Spl}_M f_a^{S_3}(X) = \mathrm{Spl}_M f_b^{S_3}(X)$ (resp. $\mathrm{Spl}_M f_{a,b}^{D_4}(X) = \mathrm{Spl}_M f_{a',b'}^{D_4}(X)$).

Kemper [Kem01], furthermore, showed that for a subgroup H of G every H-Galois extension over $M \supset k$ is also given by a specialization of $f_{\mathbf{t}}^G(X)$ as in a similar manner. Hence the following two problems naturally arise:

Field intersection problem of a generic polynomial. For a field $M \supset k$ and $\mathbf{a}, \mathbf{b} \in M^n$, determine the intersection of $\mathrm{Spl}_M f_{\mathbf{a}}^G(X)$ and $\mathrm{Spl}_M f_{\mathbf{b}}^G(X)$.

Subfield problem of a generic polynomial. For a field $M \supset k$ and $\mathbf{a}, \mathbf{b} \in M^n$, determine whether $\mathrm{Spl}_M f_{\mathbf{b}}^G(X)$ is a subfield of $\mathrm{Spl}_M f_{\mathbf{a}}^G(X)$ or not.

If we get an answer to the field intersection problem of a k-generic polynomial, we obtain an answer to the subfield problem and hence that of the field isomorphism problem.

The aim of this paper is to study a method to give an answer to the intersection problem of k-generic polynomials via formal Tschirnhausen transformation and multi-resolvent polynomials.

In Section 2, we review some known results about resolvent polynomials. In Section 3, we recall formal Tschirnhausen transformation which is given in [HM]. In Section 4, by using materials given in Sections 2 and 3, we give a general method to solve the intersection problem of k-generic polynomials.

In Section 5, we give a general method to construct a generic polynomial for the direct product $H_1 \times H_2$ of two subgroups H_1 and H_2 of S_n.

In Section 6, we take the following quintic generic polynomials with two parameters for F_{20}, D_5 and C_5, respectively, where F_{20} is the Frobenius group of order 20.

$$\begin{aligned}
f_{p,q}^{F_{20}}(X) = X^5 &+ \Big(\frac{q^2 + 5pq - 25}{p^2 + 4} - 2p + 2\Big)X^4 \\
&+ \big(p^2 - p - 3q + 5\big)X^3 + (q - 3p + 8)X^2 + (p - 6)X + 1 \ \in k(p,q)[X],
\end{aligned}$$
$$f_{s,t}^{D_5}(X) = X^5 + (t-3)X^4 + (s - t + 3)X^3 + (t^2 - t - 2s - 1)X^2 + sX + t \ \in k(s,t)[X],$$
$$h_{A,B}^{C_5}(X) = X^5 - \frac{P}{Q^2}(A^2 - 2A + 15B^2 + 2)X^3 + \frac{P^2}{Q^3}(2BX^2 - (A-1)X - 2B) \ \in k(A,B)[X]$$

where $P = (A^2 - A - 1)^2 + 25(A^2+1)B^2 + 125B^4$, $Q = 1 - A + 7B^2 + AB^2$.

Based on the general method, we illustrate the solvable quintic cases and give an explicit answer to the problem by multi-resolvent polynomials in the final Section 7. We also give some numerical examples.

2. Resolvent polynomial

In this section we review known results in the computational aspects of Galois theory (cf. the text books [Coh93], [Ade01]). One of the fundamental tools to determine the Galois group of a polynomial is the resolvent polynomials; an absolute resolvent polynomial was first introduced by Lagrange [Lag1770], and a relative resolvent polynomial by Stauduhar [Sta73]. Several kinds of methods to compute resolvent polynomials have been developed by many mathematicians (see, for example, [Sta73], [Gir83], [SM85], [Yok97], [MM97], [AV00], [GK00] and the references therein).

Let $M \supset k$ be an infinite field and $\overline{M}$ a fixed algebraic closure of M. Let $f(X) := \prod_{i=1}^{m}(X - \alpha_i) \in M[X]$ be a separable polynomial of degree m with some fixed order of the roots $\alpha_1, \ldots, \alpha_m \in \overline{M}$. The Galois group of the splitting field $\mathrm{Spl}_M f(X)$ of $f(X)$ over M may be obtained by using suitable resolvent polynomials.

Let $k[\mathbf{x}] := k[x_1, \ldots, x_m]$ be the polynomial ring over k with indeterminates $x_1, \ldots, x_m$. Put $R := k[\mathbf{x}, 1/\Delta_{\mathbf{x}}]$ where $\Delta_{\mathbf{x}} := \prod_{1 \le i < j \le m}(x_j - x_i)$. We take a surjective evaluation homomorphism $\omega_f : R \longrightarrow k(\alpha_1, \ldots, \alpha_m)$, $\Theta(x_1, \ldots, x_m) \longmapsto \Theta(\alpha_1, \ldots, \alpha_m)$, for $\Theta \in R$. We note that $\omega_f(\Delta_{\mathbf{x}}) \neq 0$ from the assumption that $f(X)$ is separable. The kernel of the map ω_f is the ideal

$$I_f = \ker(\omega_f) = \{\Theta(x_1, \ldots, x_m) \in R \mid \Theta(\alpha_1, \ldots, \alpha_m) = 0\}.$$

Let S_m be the symmetric group of degree m. For $\pi \in S_m$, we extend the action of π on m letters $\{1, \ldots, m\}$ to that on R by $\pi(\Theta(x_1, \ldots, x_m)) := \Theta(x_{\pi(1)}, \ldots, x_{\pi(m)})$. We define the Galois group of a polynomial $f(X) \in M[X]$ over M by

$$\mathrm{Gal}(f/M) := \{\pi \in S_m \mid \pi(I_f) \subseteq I_f\}.$$

We write $\mathrm{Gal}(f) := \mathrm{Gal}(f/M)$ for simplicity. The Galois group of the splitting field $\mathrm{Spl}_M f(X)$ of a polynomial $f(X)$ over M is isomorphic to $\mathrm{Gal}(f)$. If we take another ordering of roots $\alpha_{\pi(1)}, \ldots, \alpha_{\pi(m)}$ of $f(X)$ with some $\pi \in S_m$, the corresponding realization of $\mathrm{Gal}(f)$ is the conjugate of the original one given by π in S_m. Hence, for arbitrary ordering of the roots of $f(X)$, $\mathrm{Gal}(f)$ is determined up to conjugacy in S_m.

Definition. For $H \le G \le S_m$, an element $\Theta \in R$ is called a G-primitive H-invariant if $H = \mathrm{Stab}_G(\Theta) := \{\pi \in G \mid \pi(\Theta) = \Theta\}$. For a G-primitive H-invariant Θ, the polynomial

$$\mathcal{RP}_{\Theta,G}(X) := \prod_{\overline{\pi} \in G/H} (X - \pi(\Theta)) \in R^G[X]$$

where $\overline{\pi}$ runs through the left cosets on H in G, is called the *formal* G-relative H-invariant resolvent by Θ, and the polynomial

$$\mathcal{RP}_{\Theta,G,f}(X) := \prod_{\overline{\pi} \in G/H} \big(X - \omega_f(\pi(\Theta))\big)$$

is called the G-relative H-invariant resolvent of f by Θ.

The following theorem is fundamental in the theory of resolvent polynomials (cf. [Ade01, p.95]).

Theorem 2.1. *For $H \le G \le S_m$, let Θ be a G-primitive H-invariant. Assume that* $\mathrm{Gal}(f) \le G$. *Suppose that $\mathcal{RP}_{\Theta,G,f}(X)$ is decomposed into a product of powers of distinct irreducible polynomials*

as $\mathcal{RP}_{\Theta,G,f}(X)=\prod_{i=1}^{l} h_i^{e_i}(X)$ *in* $M[X]$*. Then we have a bijection*

$$\begin{array}{rcl} \mathrm{Gal}(f)\backslash G/H & \longrightarrow & \{h_1^{e_1}(X),\ldots,h_l^{e_l}(X)\} \\ \mathrm{Gal}(f)\,\pi\, H & \longmapsto & h_\pi(X)=\displaystyle\prod_{\tau H\subseteq \mathrm{Gal}(f)\,\pi\, H}\bigl(X-\omega_f(\tau(\Theta))\bigr) \end{array}$$

where the product runs through the left cosets τH *of* H *in* G *contained in* $\mathrm{Gal}(f)\,\pi\, H$*, that is, through* $\tau=\pi_\sigma\pi$ *where* π_σ *runs a system of representatives of the left cosets of* $\mathrm{Gal}(f)\cap\pi H\pi^{-1}$*; each* $h_\pi(X)$ *is irreducible or a power of an irreducible polynomial with* $\deg(h_\pi(X))=|\mathrm{Gal}(f)\,\pi\, H|/|H|$ $=|\mathrm{Gal}(f)|/|\mathrm{Gal}(f)\cap\pi H\pi^{-1}|$.

Corollary 2.2. *If* $\mathrm{Gal}(f)\le\pi H\pi^{-1}$ *for some* $\pi\in G$ *then* $\mathcal{RP}_{\Theta,G,f}(X)$ *has a linear factor over* M*. Conversely, if* $\mathcal{RP}_{\Theta,G,f}(X)$ *has a non-repeated linear factor over* M *then there exists* $\pi\in G$ *such that* $\mathrm{Gal}(f)\le\pi H\pi^{-1}$.

Remark 2.3. When the resolvent polynomial $\mathcal{RP}_{\Theta,G,f}(X)$ has a repeated factor, there always exists a suitable Tschirnhausen transformation $\hat{f}$ of f (cf. §3) over M (resp. $X-\hat{\Theta}$ of $X-\Theta$ over k) such that $\mathcal{RP}_{\Theta,G,\hat{f}}(X)$ (resp. $\mathcal{RP}_{\hat{\Theta},G,f}(X)$) has no repeated factors (cf. [Gir83], [Coh93, Alg. 6.3.4], [Col95]).

In the case where $\mathcal{RP}_{\Theta,G,f}(X)$ has no repeated factors, we have the following theorem:

Theorem 2.4. *For* $H\le G\le S_m$*, let* Θ *be a* G*-primitive* H*-invariant. We assume* $\mathrm{Gal}(f)\le G$ *and that* $\mathcal{RP}_{\Theta,G,f}(X)$ *has no repeated factors. Then the following two assertions hold*:
(i) *For* $\pi\in G$*, the fixed group of the field* $M\bigl(\omega_f(\pi(\Theta))\bigr)$ *corresponds to* $\mathrm{Gal}(f)\cap\pi H\pi^{-1}$*. In particular, the fixed group of* $\mathrm{Spl}_M\mathcal{RP}_{\Theta,G,f}(X)$ *corresponds to* $\mathrm{Gal}(f)\cap\bigcap_{\pi\in G}\pi H\pi^{-1}$;
(ii) *let* $\varphi: G\to S_{[G:H]}$ *denote the permutation representation of* G *on the left cosets of* G/H *given by the left multiplication. Then we have a realization of the Galois group of* $\mathrm{Spl}_M\mathcal{RP}_{\Theta,G,f}(X)$ *as a subgroup of* $S_{[G:H]}$ *by* $\varphi(\mathrm{Gal}(f))$.

3. Formal Tschirnhausen transformation

We recall the geometric interpretation of Tschirnhausen transformations which is given in [HM]. Let $f(X)$ be monic separable polynomial of degree n in $M[X]$ with a fixed order of the roots $\alpha_1,\ldots,\alpha_n$ of $f(X)$ in $\overline{M}$. A Tschirnhausen transformation of $f(X)$ over M is a polynomial of the form

$$g(X)=\prod_{i=1}^{n}\bigl(X-(c_0+c_1\alpha_i+\cdots+c_{n-1}\alpha_i^{n-1})\bigr),\ c_j\in M.$$

Two polynomials $f(X)$ and $g(X)$ in $M[X]$ are Tschirnhausen equivalent over M if they are Tschirnhausen transformations over M of each other. For two irreducible separable polynomials $f(X)$ and $g(X)$ in $M[X]$, $f(X)$ and $g(X)$ are Tschirnhausen equivalent over M if and only if the quotient fields $M[X]/(f(X))$ and $M[X]/(g(X))$ are isomorphic over M.

In order to obtain an answer to the field intersection problem of k-generic polynomials via multi-resolvent polynomials, we first treat a general polynomial whose roots are n indeterminates $x_1,\ldots,x_n$:

$$f_{\mathbf{s}}(X)\ =\ \prod_{i=1}^{n}(X-x_i)\ =\ X^n-s_1X^{n-1}+s_2X^{n-2}+\cdots+(-1)^ns_n\ \in k[\mathbf{s}][X]$$

where $k[x_1,\ldots,x_n]^{S_n}=k[\mathbf{s}]:=k[s_1,\ldots,s_n],\mathbf{s}=(s_1,\ldots,s_n)$, and s_i is the i-th elementary symmetric function in n variables $\mathbf{x}=(x_1,\ldots,x_n)$.

Let $R_{\mathbf{x}} := k[x_1,\ldots,x_n]$ and $R_{\mathbf{y}} := k[y_1,\ldots,y_n]$ be polynomial rings over k. Put $R_{\mathbf{x},\mathbf{y}} := k[\mathbf{x},\mathbf{y},1/\Delta_{\mathbf{x}},1/\Delta_{\mathbf{y}}]$ where $\Delta_{\mathbf{x}} := \prod_{1\leq i<j\leq n}(x_j-x_i)$ and $\Delta_{\mathbf{y}} := \prod_{1\leq i<j\leq n}(y_j-y_i)$. We define the interchanging involution $\iota_{\mathbf{x},\mathbf{y}}$ which exchanges the indeterminates x_i's and the y_i's:

$$\iota_{\mathbf{x},\mathbf{y}}\ :\ R_{\mathbf{x},\mathbf{y}} \longrightarrow R_{\mathbf{x},\mathbf{y}},\ x_i \longmapsto y_i,\ y_i \longmapsto x_i,\quad (i=1,\ldots,n). \tag{1}$$

We take another general polynomial $f_{\mathbf{t}}(X) := \iota_{\mathbf{x},\mathbf{y}}(f_{\mathbf{s}}(X)) \in k[\mathbf{t}][X], \mathbf{t} = (t_1,\ldots,t_n)$ with roots $y_1,\ldots,y_n$ where $t_i = \iota_{\mathbf{x},\mathbf{y}}(s_i)$ is the i-th elementary symmetric function in $\mathbf{y} = (y_1,\ldots,y_n)$. We put

$$K\ :=\ k(\mathbf{s},\mathbf{t});$$

it is regarded as the rational function field over k with $2n$ variables. We put $f_{\mathbf{s},\mathbf{t}}(X) := f_{\mathbf{s}}(X)f_{\mathbf{t}}(X)$. The polynomial $f_{\mathbf{s},\mathbf{t}}(X)$ of degree $2n$ is defined over K. We denote

$$G_{\mathbf{s}}\ :=\ \mathrm{Gal}(f_{\mathbf{s}}/K),\quad G_{\mathbf{t}}\ :=\ \mathrm{Gal}(f_{\mathbf{t}}/K),\quad G_{\mathbf{s},\mathbf{t}}\ :=\ \mathrm{Gal}(f_{\mathbf{s},\mathbf{t}}/K).$$

Then we have $G_{\mathbf{s},\mathbf{t}} = G_{\mathbf{s}} \times G_{\mathbf{t}}, G_{\mathbf{s}} \cong G_{\mathbf{t}} \cong S_n$ and $k(\mathbf{x},\mathbf{y})^{G_{\mathbf{s},\mathbf{t}}} = K$.

We intend to apply the results of the previous section for $m = 2n, G = G_{\mathbf{s},\mathbf{t}} \leq S_{2n}$ and $f = f_{\mathbf{s},\mathbf{t}}$.

Note that over the field $\mathrm{Spl}_K f_{\mathbf{s},\mathbf{t}}(X) = k(\mathbf{x},\mathbf{y})$, there exist $n!$ Tschirnhausen transformations from $f_{\mathbf{s}}(X)$ to $f_{\mathbf{t}}(X)$ with respect to $y_{\pi(1)},\ldots,y_{\pi(n)}$ for $\pi \in S_n$. We study the field of definition of each Tschirnhausen transformation from $f_{\mathbf{s}}(X)$ to $f_{\mathbf{t}}(X)$. Let

$$D := \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

be the Vandermonde matrix of size n. The matrix $D \in M_n(k(\mathbf{x}))$ is invertible because the determinant of D equals $\det D = \Delta_{\mathbf{x}}$. When $\mathrm{char}\, k \neq 2$, the field $k(\mathbf{s})(\Delta_{\mathbf{x}})$ is a quadratic extension of $k(\mathbf{s})$ which corresponds to the fixed field of the alternating group of degree n. We define the n-tuple $(u_0(\mathbf{x},\mathbf{y}),\ldots,u_{n-1}(\mathbf{x},\mathbf{y})) \in (R_{\mathbf{x},\mathbf{y}})^n$ by

$$\begin{pmatrix} u_0(\mathbf{x},\mathbf{y}) \\ u_1(\mathbf{x},\mathbf{y}) \\ \vdots \\ u_{n-1}(\mathbf{x},\mathbf{y}) \end{pmatrix} := D^{-1} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}. \tag{2}$$

Cramer's rule shows

$$u_i(\mathbf{x},\mathbf{y}) = \Delta_{\mathbf{x}}^{-1} \cdot \det \begin{pmatrix} 1 & x_1 & \cdots & x_1^{i-1} & y_1 & x_1^{i+1} & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{i-1} & y_2 & x_2^{i+1} & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{i-1} & y_n & x_n^{i+1} & \cdots & x_n^{n-1} \end{pmatrix}. \tag{3}$$

In order to simplify the presentation, we write

$$u_i := u_i(\mathbf{x},\mathbf{y}),\quad (i=0,\ldots,n-1).$$

The Galois group $G_{\mathbf{s},\mathbf{t}}$ acts on the orbit $\{\pi(u_i) \mid \pi \in G_{\mathbf{s},\mathbf{t}}\}$ via regular representation from the left. However this action is not faithful. We put

$$H_{\mathbf{s},\mathbf{t}} := \{(\pi_{\mathbf{x}},\pi_{\mathbf{y}}) \in G_{\mathbf{s},\mathbf{t}} \mid \pi_{\mathbf{x}}(i) = \pi_{\mathbf{y}}(i) \text{ for } i=1,\ldots,n\} \cong S_n.$$

If $\pi \in H_{\mathbf{s},\mathbf{t}}$ then we have $\pi(u_i) = u_i$ for $i = 0,\ldots,n-1$. Indeed we see the following lemma:

Lemma 3.1. *For i, $0 \leq i \leq n-1$, u_i is a $G_{\mathbf{s},\mathbf{t}}$-primitive $H_{\mathbf{s},\mathbf{t}}$-invariant.*

Let $\Theta := \Theta(\mathbf{x},\mathbf{y})$ be a $G_{\mathbf{s},\mathbf{t}}$-primitive $H_{\mathbf{s},\mathbf{t}}$-invariant. Let $\overline{\pi} = \pi H_{\mathbf{s},\mathbf{t}}$ be a left coset of $H_{\mathbf{s},\mathbf{t}}$ in $G_{\mathbf{s},\mathbf{t}}$. The group $G_{\mathbf{s},\mathbf{t}}$ acts on the set $\{\pi(\Theta) \mid \overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}\}$ transitively from the left through the action on the set $G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$ of left cosets. Each of the sets $\{\overline{(1,\pi_{\mathbf{y}})} \mid (1,\pi_{\mathbf{y}}) \in G_{\mathbf{s},\mathbf{t}}\}$ and $\{\overline{(\pi_{\mathbf{x}},1)} \mid (\pi_{\mathbf{x}},1) \in G_{\mathbf{s},\mathbf{t}}\}$ forms a complete residue system of $G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$, and hence the subgroups $G_{\mathbf{s}}$ and $G_{\mathbf{t}}$ of $G_{\mathbf{s},\mathbf{t}}$ act on the set $\{\pi(\Theta) \mid \overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}\}$ transitively. For $\overline{\pi} = \overline{(1,\pi_{\mathbf{y}})} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$, we obtain the following equality from the definition (2):

$$y_{\pi_{\mathbf{y}}(i)} = \pi_{\mathbf{y}}(u_0) + \pi_{\mathbf{y}}(u_1)x_i + \cdots + \pi_{\mathbf{y}}(u_{n-1})x_i^{n-1} \text{ for } i = 1,\ldots,n.$$

Hence the set $\{(\pi(u_0),\ldots,\pi(u_{n-1})) \mid \overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}\}$ gives coefficients of $n!$ different Tschirnhausen transformations from $f_{\mathbf{s}}(X)$ to $f_{\mathbf{t}}(X)$ each of which is defined over $K(\pi(u_0),\ldots,\pi(u_{n-1}))$, respectively. We call $K(\pi(u_0),\ldots,\pi(u_{n-1})), (\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}})$, a field of formal Tschirnhausen coefficients from $f_{\mathbf{s}}(X)$ to $f_{\mathbf{t}}(X)$. We put $v_i := \iota_{\mathbf{x},\mathbf{y}}(u_i)$ for $i = 0,\ldots,n-1$. Then v_i is also a $G_{\mathbf{s},\mathbf{t}}$-primitive $H_{\mathbf{s},\mathbf{t}}$-invariant and $K(\pi(v_0),\ldots,\pi(v_{n-1}))$ gives a field of formal Tschirnhausen coefficients from $f_{\mathbf{t}}(X)$ to $f_{\mathbf{s}}(X)$.

Proposition 3.2. *Let Θ be a $G_{\mathbf{s},\mathbf{t}}$-primitive $H_{\mathbf{s},\mathbf{t}}$-invariant. Then we have $k(\mathbf{x},\mathbf{y})^{\pi H_{\mathbf{s},\mathbf{t}}\pi^{-1}} = K(\pi(u_0),\ldots,\pi(u_{n-1})) = K(\pi(\Theta))$ and $[K(\pi(\Theta)) : K] = n!$ for each $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$.*

Hence, for each of the $n!$ fields $K(\pi(\Theta))$, we have $\mathrm{Spl}_{K(\pi(\Theta))}f_{\mathbf{s}}(X) = \mathrm{Spl}_{K(\pi(\Theta))}f_{\mathbf{t}}(X), (\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}})$. We also obtain the following proposition:

Proposition 3.3. *Let Θ be a $G_{\mathbf{s},\mathbf{t}}$-primitive $H_{\mathbf{s},\mathbf{t}}$-invariant. Then we have*

(i) $K(\mathbf{x}) \cap K(\pi(\Theta)) = K(\mathbf{y}) \cap K(\pi(\Theta)) = K$ *for* $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$;

(ii) $K(\mathbf{x},\mathbf{y}) = K(\mathbf{x},\pi(\Theta)) = K(\mathbf{y},\pi(\Theta))$ *for* $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$;

(iii) $K(\mathbf{x},\mathbf{y}) = K(\pi(\Theta) \mid \overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}})$.

We consider the formal $G_{\mathbf{s},\mathbf{t}}$-relative $H_{\mathbf{s},\mathbf{t}}$-invariant resolvent polynomial of degree $n!$ by Θ:

$$\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}}}(X) = \prod_{\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}} (X - \pi(\Theta)) \in k(\mathbf{s},\mathbf{t})[X].$$

It follows from Proposition 3.2 that $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}}}(X)$ is irreducible over $k(\mathbf{s},\mathbf{t})$. From Proposition 3.3 we have one of the basic results:

Theorem 3.4. *The polynomial $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}}}(X)$ is k-generic for $S_n \times S_n$.*

4. Field intersection problem

For $\mathbf{a} = (a_1,\ldots,a_n), \mathbf{b} = (b_1,\ldots,b_n) \in M^n$, we take some fixed order of the roots $\alpha_1,\ldots,\alpha_n$ (resp. $\beta_1,\ldots,\beta_n$) of $f_{\mathbf{a}}(X)$ (resp. $f_{\mathbf{b}}(X)$) in $\overline{M}$. Put $f_{\mathbf{a},\mathbf{b}}(X) := f_{\mathbf{a}}(X)f_{\mathbf{b}}(X) \in M[X]$. We denote $L_{\mathbf{a}} := M(\alpha_1,\ldots,\alpha_n)$ and $L_{\mathbf{b}} := M(\beta_1,\ldots,\beta_n)$; then $L_{\mathbf{a}} = \mathrm{Spl}_M f_{\mathbf{a}}(X)$, $L_{\mathbf{b}} = \mathrm{Spl}_M f_{\mathbf{b}}(X)$ and $L_{\mathbf{a}}\,L_{\mathbf{b}} = \mathrm{Spl}_M f_{\mathbf{a},\mathbf{b}}(X)$. We define a specialization homomorphism $\omega_{f_{\mathbf{a},\mathbf{b}}}$ by

$$\begin{aligned}\omega_{f_{\mathbf{a},\mathbf{b}}} : R_{\mathbf{x},\mathbf{y}} &\longrightarrow M(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n) = L_{\mathbf{a}}\,L_{\mathbf{b}},\\ \Theta(\mathbf{x},\mathbf{y}) &\longmapsto \Theta(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n).\end{aligned}$$

Denote $\Delta_{\mathbf{a}} := \omega_{f_{\mathbf{a},\mathbf{b}}}(\Delta_{\mathbf{x}})$ and $\Delta_{\mathbf{b}} := \omega_{f_{\mathbf{a},\mathbf{b}}}(\Delta_{\mathbf{y}})$. We assume that both of the polynomials $f_{\mathbf{a}}(X)$ and $f_{\mathbf{b}}(X)$ are separable over M, i.e. $\omega_{f_{\mathbf{a},\mathbf{b}}}(\Delta_{\mathbf{x}}) \cdot \omega_{f_{\mathbf{a},\mathbf{b}}}(\Delta_{\mathbf{y}}) \neq 0$. Put

$$G_{\mathbf{a}} := \mathrm{Gal}(f_{\mathbf{a}}/M), \quad G_{\mathbf{b}} := \mathrm{Gal}(f_{\mathbf{b}}/M), \quad G_{\mathbf{a},\mathbf{b}} := \mathrm{Gal}(f_{\mathbf{a},\mathbf{b}}/M).$$

Then we may naturally regard $G_{\mathbf{a},\mathbf{b}}$ as a subgroup of $G_{\mathbf{s},\mathbf{t}}$. For $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$, we put $c_{i,\pi} := \omega_{f_{\mathbf{a},\mathbf{b}}}(\pi(u_i)), d_{i,\pi} := \omega_{f_{\mathbf{a},\mathbf{b}}}\big(\pi(\iota_{\mathbf{x},\mathbf{y}}(u_i))\big)$, $(i = 0,\ldots,n-1)$. Then we have

$$\beta_{\pi_{\mathbf{y}}(i)} \;=\; c_{0,\pi} + c_{1,\pi}\,\alpha_{\pi_{\mathbf{x}}(i)} + \cdots + c_{n-1,\pi}\,\alpha_{\pi_{\mathbf{x}}(i)}^{n-1}, \tag{4}$$

$$\alpha_{\pi_{\mathbf{x}}(i)} \;=\; d_{0,\pi} + d_{1,\pi}\,\beta_{\pi_{\mathbf{y}}(i)} + \cdots + d_{n-1,\pi}\,\beta_{\pi_{\mathbf{y}}(i)}^{n-1} \tag{5}$$

for each $i = 1, \ldots, n$.

For each $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$, there exists a Tschirnhausen transformation from $f_{\mathbf{a}}(X)$ to $f_{\mathbf{b}}(X)$ over its field of Tschirnhausen coefficients $M(c_{0,\pi}, \ldots, c_{n-1,\pi})$; the n-tuple $(d_{0,\pi}, \ldots, d_{n-1,\pi})$ gives the coefficients of a transformation of the inverse direction. From the assumption $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$, we see the following lemma (cf. [JLY02, p. 141], [HM]):

Lemma 4.1. *Let M'/M be a field extension. If $f_{\mathbf{b}}(X)$ is a Tschirnhausen transformation of $f_{\mathbf{a}}(X)$ over M', then $f_{\mathbf{a}}(X)$ is a Tschirnhausen transformation of $f_{\mathbf{b}}(X)$ over M'. In particular, we have $M(c_{0,\pi}, \ldots, c_{n-1,\pi}) = M(d_{0,\pi}, \ldots, d_{n-1,\pi})$ for every $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$.*

In order to obtain an answer to the field intersection problem of $f_{\mathbf{s}}(X)$ we study the $n!$ fields $M(c_{0,\pi}, \ldots, c_{n-1,\pi})$ of Tschirnhausen coefficients from $f_{\mathbf{a}}(X)$ to $f_{\mathbf{b}}(X)$ over M.

Proposition 4.2. *Under the assumption $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$, we have the following two assertions:*

(i) $\mathrm{Spl}_{M(c_{0,\pi},\ldots,c_{n-1,\pi})} f_{\mathbf{a}}(X) = \mathrm{Spl}_{M(c_{0,\pi},\ldots,c_{n-1,\pi})} f_{\mathbf{b}}(X)$ *for each* $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$;

(ii) $L_{\mathbf{a}} L_{\mathbf{b}} = L_{\mathbf{a}}\, M(c_{0,\pi}, \ldots, c_{n-1,\pi}) = L_{\mathbf{b}}\, M(c_{0,\pi}, \ldots, c_{n-1,\pi})$ *for each* $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$.

Let $\Theta = \Theta(\mathbf{x}, \mathbf{y})$ be a $G_{\mathbf{s},\mathbf{t}}$-primitive $H_{\mathbf{s},\mathbf{t}}$-invariant. Applying the specialization $\omega_{f_{\mathbf{a},\mathbf{b}}}$ to Θ, we have a $G_{\mathbf{s},\mathbf{t}}$-relative $H_{\mathbf{s},\mathbf{t}}$-invariant resolvent polynomial of $f_{\mathbf{a},\mathbf{b}}$ by Θ:

$$\mathcal{RP}_{\Theta, G_{\mathbf{s},\mathbf{t}}, f_{\mathbf{a},\mathbf{b}}}(X) = \prod_{\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}} \big(X - \omega_{f_{\mathbf{a},\mathbf{b}}}(\pi(\Theta))\big) \in M[X].$$

The resolvent polynomial $\mathcal{RP}_{\Theta, G_{\mathbf{s},\mathbf{t}}, f_{\mathbf{a},\mathbf{b}}}(X)$ is also called (absolute) multi-resolvent (cf. [GLV88], [RV99], [Val], [Ren04]).

Proposition 4.3. *For $\mathbf{a}, \mathbf{b} \in M^n$ with $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$, suppose that the resolvent polynomial $\mathcal{RP}_{\Theta, G_{\mathbf{s},\mathbf{t}}, f_{\mathbf{a},\mathbf{b}}}(X)$ has no repeated factors. Then the following two assertions hold:*
(i) $M(c_{0,\pi}, \ldots, c_{n-1,\pi}) = M\big(\omega_{f_{\mathbf{a},\mathbf{b}}}(\pi(\Theta))\big)$ *for each* $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$;
(ii) $\mathrm{Spl}_M f_{\mathbf{a},\mathbf{b}}(X) = M(\omega_{f_{\mathbf{a},\mathbf{b}}}(\pi(\Theta)) \mid \overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}})$.

Definition. For a separable polynomial $f(X) \in k[X]$ of degree d, the decomposition type of $f(X)$ over M, denoted by $\mathrm{DT}(f/M)$, is defined as the partition of d induced by the degrees of the irreducible factors of $f(X)$ over M. We define the decomposition type $\mathrm{DT}(\mathcal{RP}_{\Theta,G,f}/M)$ of $\mathcal{RP}_{\Theta,G,f}(X)$ over M by $\mathrm{DT}(\mathcal{RP}_{\Theta,G,\hat{f}}/M)$ where $\hat{f}(X)$ is a Tschirnhausen transformation of $f(X)$ over M which satisfies that $\mathcal{RP}_{\Theta,G,\hat{f}}(X)$ has no repeated factors (cf. Remark 2.3).

We write $\mathrm{DT}(f) := \mathrm{DT}(f/M)$ for simplicity. From Theorem 2.1, the decomposition type $\mathrm{DT}(\mathcal{RP}_{\Theta, G_{\mathbf{s},\mathbf{t}}, f_{\mathbf{a},\mathbf{b}}})$ coincides with the partition of $n!$ induced by the lengths of the orbits of $G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$ under the action of $\mathrm{Gal}(f_{\mathbf{a},\mathbf{b}})$.

Hence, by Proposition 4.3, $\mathrm{DT}(\mathcal{RP}_{\Theta, G_{\mathbf{s},\mathbf{t}}, f_{\mathbf{a},\mathbf{b}}})$ gives the degrees of $n!$ fields of Tschirnhausen coefficients $M(c_{0,\pi}, \ldots, c_{n-1,\pi})$ from $f_{\mathbf{a}}(X)$ to $f_{\mathbf{b}}(X)$ over M; the degree of $M(c_{0,\pi}, \ldots, c_{n-1,\pi})$ over M is equal to $|\mathrm{Gal}(f_{\mathbf{a},\mathbf{b}})|/|\mathrm{Gal}(f_{\mathbf{a},\mathbf{b}}) \cap \pi H_{\mathbf{s},\mathbf{t}} \pi^{-1}|$.

We conclude that the decomposition type of the resolvent polynomial $\mathcal{RP}_{\Theta, G_{\mathbf{s},\mathbf{t}}, f_{\mathbf{a},\mathbf{b}}}(X)$ over M gives us information about the field intersection problem of $f_{\mathbf{s}}(X)$ through the degrees of the fields of Tschirnhausen coefficients $M(c_{0,\pi}, \ldots, c_{n-1,\pi})$ over M which is determined by the degeneration of the Galois group $\mathrm{Gal}(f_{\mathbf{a},\mathbf{b}})$ under the specialization $(\mathbf{s}, \mathbf{t}) \mapsto (\mathbf{a}, \mathbf{b})$.

Theorem 4.4. *Let Θ be a $G_{\mathbf{s},\mathbf{t}}$-primitive $H_{\mathbf{s},\mathbf{t}}$-invariant. For $\mathbf{a}, \mathbf{b} \in M^n$ with $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$, the following three conditions are equivalent:*
(1) *$M[X]/(f_{\mathbf{a}}(X))$ and $M[X]/(f_{\mathbf{b}}(X))$ are M-isomorphic;*
(2) *There exists $\pi \in G_{\mathbf{s},\mathbf{t}}$ such that $\omega_{f_{\mathbf{a},\mathbf{b}}}(\pi(\Theta)) \in M$;*
(3) *The decomposition type $\mathrm{DT}(\mathcal{RP}_{\Theta, G_{\mathbf{s},\mathbf{t}}, f_{\mathbf{a},\mathbf{b}}})$ over M includes 1.*

In the case where $G_{\mathbf{a}}$ and $G_{\mathbf{b}}$ are isomorphic to a transitive subgroup G of S_n and every subgroups of G with index n are conjugate in G, the condition that $M[X]/(f_{\mathbf{a}}(X))$ and $M[X]/(f_{\mathbf{b}}(X))$ are M-isomorphic is equivalent to the condition that $\mathrm{Spl}_M f_{\mathbf{a}}(X)$ and $\mathrm{Spl}_M f_{\mathbf{b}}(X)$ coincide. Hence we obtain an answer to the field isomorphism problem via the resolvent polynomial $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}}(X)$.

Corollary 4.5 (The field isomorphism problem). *For $\mathbf{a},\mathbf{b}\in M^n$ with $\Delta_{\mathbf{a}}\cdot\Delta_{\mathbf{b}}\neq 0$, we assume that both of $f_{\mathbf{a}}(X)$ and $f_{\mathbf{b}}(X)$ are irreducible over M, that $G_{\mathbf{a}}$ and $G_{\mathbf{b}}$ are isomorphic to G and that all subgroups of G with index n are conjugate in G. Then $\mathrm{DT}(\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}})$ includes 1 if and only if $\mathrm{Spl}_M f_{\mathbf{a}}(X)$ and $\mathrm{Spl}_M f_{\mathbf{b}}(X)$ coincide.*

Remark 4.6. If G is one of the symmetric group S_n of degree n, $(n\neq 6)$, the alternating group of degree n, $(n\neq 6)$, and solvable transitive subgroups of S_p of prime degree p, then all subgroups of G with index n or p, respectively, are conjugate in G (cf. [Hup67], [BJY86]).

Example 4.7. In the case where $G\leq S_n$ has r conjugacy classes of subgroups of index n, we get an answer to the field isomorphism problem by applying Theorem 4.4 repeatedly.

For example, when char $k\neq 2$, the polynomials $f_{\mathbf{s}}(X):=f_{s,t}^{D_4}(X)=X^4+sX^2+t$ and $g_{\mathbf{s}}(X):=g_{s,t}^{D_4}(X)=X^4+2sX^2+(s^2-4t)$, $\mathbf{s}=(s,t)$, are k-generic for D_4 and have the same splitting field over $k(s,t)$. However their root fields are not isomorphic over $k(s,t)$.

For $\mathbf{a}=(a,b)$, $\mathbf{a}'=(a',b')\in M^2$ with $G_{\mathbf{a}}=G_{\mathbf{a}'}=D_4$, we see that $\mathrm{Spl}_M f_{\mathbf{a}}(X)=\mathrm{Spl}_M f_{\mathbf{a}'}(X)$ if and only if either $M[X]/(f_{\mathbf{a}}(X))\cong_M M[X]/(f_{\mathbf{a}'}(X))$ or $M[X]/(f_{\mathbf{a}}(X))\cong_M M[X]/(g_{\mathbf{a}'}(X))$. Hence, by applying Theorem 4.4 twice, we obtain an answer to the field isomorphism problem.

The decomposition types of the corresponding multi-resolvent polynomials $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a}}f_{\mathbf{a}'}}(X)$ and $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a}}g_{\mathbf{a}'}}(X)$ are given as $8,4,4,2,2,2,1,1$ and $8,8,4,2,2$. Note, in this case, that the latter decomposition type also means the isomorphism of the two splitting fields of $f_{\mathbf{a}}(X)$ and of $f_{\mathbf{a}'}(X)$ over M although it does not include 1 (cf. [HM-2]).

5. Generic polynomial for $H_1\times H_2$

Let H_1 and H_2 be subgroups of S_n. As an analogue to Theorem 3.4, we obtain a k-generic polynomial for $H_1\times H_2$, the direct product of groups H_1 and H_2.

Theorem 5.1. *Let $M=k(q_1,\ldots,q_l,r_1,\ldots,r_m)$, $(1\leq l,m\leq n-1)$ be the rational function field over k with $(l+m)$ variables. For $\mathbf{a}\in k(q_1,\ldots,q_l)^n,\mathbf{b}\in k(r_1,\ldots,r_m)^n$, we assume that $f_{\mathbf{a}}(X)\in M[X]$ and $f_{\mathbf{b}}(X)\in M[X]$ be k-generic polynomials for H_1 and H_2, respectively. If $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}}(X)\in M[X]$ has no repeated factors, then $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}}(X)$ is a k-generic polynomial for $H_1\times H_2$ which is not necessary irreducible.*

Example 5.2. In each Tschirnhausen equivalence class, we are always able to choose a specialization $\mathbf{s}\mapsto\mathbf{a}\in M^n$ of the polynomial $f_{\mathbf{s}}(X)$ which satisfy $a_1=0$ and $a_{n-1}=a_n$ (see [JLY02, §8.2]). Thus the polynomial

$$X^n+q_2X^{n-2}+\cdots+q_{n-2}X^2+q_{n-1}X+q_{n-1}$$

is k-generic for S_n with $(n-2)$ parameters $q_2,\ldots,q_{n-1}$ over an arbitrary field k. For $M=k(q_2,\ldots,q_{n-1},r_2,\ldots,r_{n-1})$, we take $\mathbf{a}=(0,q_2,\ldots,q_{n-1},q_{n-1})\in M^n,\mathbf{b}=(0,r_2,\ldots,r_{n-1},r_{n-1})\in M^n$. While the polynomial $f_{\mathbf{a}}(X)f_{\mathbf{b}}(X)$ of degree $2n$ is k-generic for $S_n\times S_n$, the resolvent polynomial $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}}(X)$ (with no repeated factors) realizes an irreducible k-generic polynomial for $S_n\times S_n$ of degree $n!$.

Example 5.3. In the case of $n=3$, some explicit examples of sextic k-generic polynomials $f_{s,t}^{H_1\times H_2}(X)$ for transitive subgroups $H_1\times H_2$ of S_6 are given in [HM]. We give another examples by taking $\Theta=x_1y_1+x_2y_2+x_3y_3$, $f_s^{S_3}(X)=X^3+sX+s$, $f_s^{C_3}(X)=X^3-sX^2-(s+3)X-1$,

$f_s^{C_2}(X) = X(X^2 - s)$, $f_s^{\{1\}}(X) = X(X^2-1)$ when char $k \neq 3$. Then we get the following k-generic polynomials $h^{H_1,H_2}(X) := \mathcal{RP}_{\Theta, G_{\mathbf{s},\mathbf{t}}, f_s^{H_1} f_t^{H_2}}(X)$ for $H_1 \times H_2$:

$$\begin{aligned}
h^{S_3,S_3}(X) &= X^6 - 6stX^4 - 27stX^3 + 9s^2t^2X^2 + 81s^2t^2X - s^2t^2(4st + 27s + 27t),\\
h^{S_3,C_3}(X) &= X^6 + 2s(t^2+3t+9)X^4 + s(2t+3)(t^2+3t+9)X^3 + s^2(t^2+3t+9)^2X^2\\
&\qquad + s^2(2t+3)(t^2+3t+9)^2X + s^2(t^2+3t+9)^2(t^2+3t+s+9),\\
h^{S_3,C_2}(X) &= X^6 + 6stX^4 + 9s^2t^2X^2 + s^2t^3(4s+27),\\
h^{S_3,\{1\}}(X) &= X^6 + 6sX^4 + 9s^2X^2 + s^2(4s+27),\\
h^{C_3,C_2}(X) &= X^6 - 2t(s^2+3s+9)X^4 + t^2(s^2+3s+9)^2X^2 - t^3(s^2+3s+9)^2.
\end{aligned}$$

6. Solvable quintic generic polynomial

We recall some solvable quintic generic polynomials (cf. [Lec98], [JLY02], [HT03]). Let $\sigma := (12345)$, $\rho := (1243)$, $\tau := \rho^2$, $\omega := (12) \in S_5$ acting on $k(x_1, \ldots, x_5)$ by $\pi(x_i) = x_{\pi(i)}, (\pi \in S_5)$. For simplicity, in this section, we write

$$C_5 = \langle \sigma \rangle, \quad D_5 = \langle \sigma, \tau \rangle, \quad F_{20} = \langle \sigma, \rho \rangle, \quad S_5 = \langle \sigma, \omega \rangle,$$

where C_5 (resp. D_5, F_{20}, S_5) is the cyclic (resp. dihedral, Frobenius, symmetric) group of order 5 (resp. 10, 20, 120). Put

$$x := \left(\frac{x_1 - x_4}{x_1 - x_3}\right) \Big/ \left(\frac{x_2 - x_4}{x_2 - x_3}\right), \quad y := \left(\frac{x_2 - x_5}{x_2 - x_4}\right) \Big/ \left(\frac{x_3 - x_5}{x_3 - x_4}\right). \tag{6}$$

Then the symmetric group S_5 of degree 5 faithfully acts on $k(x,y)$ in the manner,

$$\begin{aligned}
&\sigma \;:\; x \longmapsto y, \quad y \longmapsto -\frac{y-1}{x}, && \tau \;:\; x \longmapsto x, \quad y \longmapsto -\frac{x-1}{y},\\
&\rho \;:\; x \longmapsto \frac{x}{x-1}, \quad y \longmapsto \frac{y-1}{x+y-1}, && \omega \;:\; x \longmapsto \frac{1}{x}, \quad y \longmapsto \frac{x+y-1}{x}.
\end{aligned} \tag{7}$$

We take a D_5-primitive $\langle \tau \rangle$-invariant x and have

$$\{\pi(x) \mid \overline{\pi} \in D_5/\langle \tau \rangle\} = \left\{x, y, -\frac{y-1}{x}, \frac{x+y-1}{xy}, -\frac{x-1}{y}\right\}.$$

Hence we obtain the formal D_5-relative $\langle \tau \rangle$-invariant resolvent polynomial by x,

$$\begin{aligned}
f_{s,t}^{D_5}(X) := \mathcal{RP}_{x,D_5}(X) &= \prod_{\overline{\pi} \in D_5/\langle \tau \rangle} (X - \pi(x))\\
&= X^5 + (t-3)X^4 + (s-t+3)X^3 + (t^2 - t - 2s - 1)X^2 + sX + t \;\in\; k(s,t)[X]
\end{aligned}$$

where

$$\begin{aligned}
t &:= -\frac{(x-1)(y-1)(x+y-1)}{xy},\\
s &:= \sum_{i=0}^{4} \sigma^i\big((x-1)(y-1)\big) \qquad (8)\\
&= -(x - 2x^2 + x^3 + y - 4xy + 5x^2y - 3x^3y + x^4y - 2y^2 + 5xy^2\\
&\qquad - 5x^2y^2 + 2x^3y^2 + y^3 - 3xy^3 + 2x^2y^3 - x^3y^3 + xy^4)/(x^2y^2).
\end{aligned}$$

Note that $k(x,y)^{D_5} = k(s,t)$. By the normal basis theorem and Remark 2.3, we see that the polynomial $f_{s,t}^{D_5}(X) \in k(s,t)[X]$ is a k-generic polynomial for D_5 (cf. [JLY02, p. 45]). The

polynomial $f_{s,t}^{D_5}(X)$ is known as Brumer's quintic. Put

$$\begin{aligned} d &:= \prod_{\overline{\pi}\in D_5/\langle\tau\rangle} (\pi(x)-\pi^2(x)) \\ &= \frac{(x-y)(x+xy-1)(y+xy-1)(x^2+y-1)(x+y^2-1)}{x^3y^3}; \end{aligned}$$

then d satisfies the relation

$$d^2=\delta_{s,t} := s^2-4s^3+4t-14st-30s^2t-91t^2-34st^2+s^2t^2+40t^3+24st^3+4t^4-4t^5. \tag{9}$$

We note that the discriminant of $f_{s,t}^{D_5}(X)$ with respect to X is given by $t^2\delta_{s,t}^2$. In the case of char $k\neq 2$, we also see $k(x,y)^{C_5}=k(s,t)(d)$; the field $k(s,t,d)$ is a quadratic subextension of $k(x,y)$ over $k(s,t)$. By blowing up the surface (9), Hashimoto-Tsunogai [HT03] showed that the fixed field $k(x,y)^{C_5}=k(s,t,d)$ is purely transcendental over k. A minimal basis of $k(x,y)^{C_5}=k(A,B)$ over k is given explicitly by

$$A=\frac{s+13t-7st-2t^2+2t^3}{-2+7s+33t+st-8t^2},\quad B=\frac{d}{-2+7s+33t+st-8t^2}.$$

We also see

$$s=\frac{2A+13t-33At-2t^2+8At^2+2t^3}{-1+7A+7t+At},\quad d=\frac{2B(-1-11t+t^2)^2}{-1+7A+7t+At} \tag{10}$$

and

$$t=-\frac{A^2+A^3-B^2+7AB^2}{1-A+7B^2+AB^2}. \tag{11}$$

Hence we obtain the generating polynomial of the field $k(x,y)$ over $k(x,y)^{C_5}=k(A,B)$:

$$f_{A,B}^{C_5}(X) := f_{s,t}^{D_5}(X)\in k(A,B)[X] \tag{12}$$

where $s,t\in k(A,B)$ are given by the above formulas (10) and (11). The polynomial $f_{A,B}^{C_5}(X)$ is k-generic for C_5 with independent parameters A,B when char $k\neq 2$. The discriminant of $f_{A,B}^{C_5}(X)$ with respect to X is given by

$$\frac{16B^4(A^2+A^3-B^2+7AB^2)^2P^8}{Q^{14}}$$

where

$$P=(A^2-A-1)^2+25(A^2+1)B^2+125B^4,\quad Q=1-A+7B^2+AB^2. \tag{13}$$

We also get an alternative presentation of the k-generic polynomial $f_{A,B}^{C_5}(X)$ as

$$\begin{aligned} g_{s,t}^{C_5}(X) &:= \mathcal{RP}_{x-y,C_5}(X) \\ &= X^5-(2-3s-2t+t^2)X^3+dX^2+(1-3s-10t-4st+3t^2+t^3)X-d. \end{aligned}$$

By using $s,t,d\in k(A,B)$ in (10) and (11), we have the following k-generic polynomial (cf. [HT03]):

$$\begin{aligned} h_{A,B}^{C_5}(X) &:= g_{s,t}^{C_5}(X) \\ &= X^5-\frac{P}{Q^2}(A^2-2A+15B^2+2)X^3+\frac{P^2}{Q^3}(2BX^2-(A-1)X-2B) \end{aligned}$$

where $P,Q\in k(A,B)$ are given as in (13) above.

We note that two polynomials $f_{A,B}^{C_5}(X)$ and $h_{A,B}^{C_5}(X)$ have the same splitting field $k(x,y)$ over $k(A,B)$. The actions of ρ and of $\tau=\rho^2$ on the fields $k(x,y)^{C_5}=k(s,t,d)=k(A,B)$ and $k(x,y)^{D_5}=k(s,t)$ are given by

$$\begin{aligned}\rho\ &:\ s\longmapsto\frac{s+5t}{t^2},\quad t\longmapsto-\frac{1}{t},\quad d\longmapsto\frac{d}{t^3},\quad A\longmapsto-\frac{1}{A},\quad B\longmapsto-\frac{B}{A},\\ \tau\ &:\ s\longmapsto s,\quad t\longmapsto t,\quad d\longmapsto -d,\quad A\longmapsto A,\quad B\longmapsto -B.\end{aligned}\tag{14}$$

Proposition 6.1. *Assume that char $k\neq 2$.*
(1) *The polynomials $h_{A,B}^{C_5}(X)$, $h_{-1/A,-B/A}^{C_5}(X)$, $h_{A,-B}^{C_5}(X)$ and $h_{-1/A,B/A}^{C_5}(X)$ have the same splitting field $k(x,y)$ over $k(A,B)$.*
(2) *The polynomials $f_{s,t}^{D_5}(X)$ and $f_{(s+5t)/t^2,-1/t}^{D_5}(X)$ have the same splitting field $k(x,y)$ over $k(s,t)$.*

Proof. (1) Since $f_{\rho^i(A),\rho^i(B)}^{C_5}(X)=\mathcal{RP}_{\rho^i(x),D_5}(X)$, $(i=1,2,3)$, each of $\rho^i(x)$, $(i=1,2,3)$ is a D_5-primitive $\langle\tau\rangle$-invariant. Hence the polynomial $f_{A,B}^{C_5}(X)$ and $f_{\rho^i(A),\rho^i(B)}^{C_5}(X)$ have the same splitting field $k(x,y)$ over $k(A,B)$. The assertion now follows because the splitting fields of $f_{A,B}^{C_5}(X)$ and of $h_{A,B}^{C_5}(X)$ over $k(A,B)$ coincide.
(2) The assertion follows from $f_{\rho(s),\rho(t)}^{D_5}(X)=\mathcal{RP}_{\rho(x),D_5}(X)$ because $\rho(x)$ is a D_5-primitive $\langle\tau\rangle$-invariant. □

Example 6.2. In Proposition 6.1, if we specialize the parameter $t:=1$, then we see two polynomials

$$\begin{aligned}f_s^1(X)&:=f_{s,1}^{D_5}(X)=X^5-2X^4+(s+2)X^3-(2s+1)X^2+sX+1,\\ f_s^2(X)&:=f_{s+5,-1}^{D_5}(X)=X^5-4X^4+(s+9)X^3-(2s+9)X^2+(s+5)X-1\end{aligned}$$

have the same splitting field over $k(s)$ including the quadratic field $k(s)(\sqrt{47+24s+28s^2+4s^3})$ of $k(s)$. Now we take a base field M as a number field K and take an algebraic integer $s_1\in K$. Note that if x is a root of $f_{s_1,1}^{D_5}(X)$ then $\rho(x)=x/(x-1)$ is a root of $f_{s_1+5,-1}^{D_5}(X)$. Put

$$\begin{aligned}g_{s_1}^1(Y)&:=Y^5\cdot f_{-s_1}^1(1/Y)=Y^5-s_1Y^4+(2s_1-1)Y^3-(s_1-2)Y^2-2Y+1,\\ g_{s_1}^2(Y)&:=(-Y)^5\cdot f_{-s_1}^2(-1/Y)=Y^5-(s_1-5)Y^4-(2s_1-9)Y^3-(s_1-9)Y^2+4Y+1.\end{aligned}$$

Then we have $g_{s_1}^1(Y)=g_{s_1}^2(Y-1)$; hence, if θ is a root of $g_{s_1}^1(X)$ then $\theta-1$ is a root of $g_{s_1}^2(X)$. In particular, both of θ and $\theta-1$ are units in the same quintic cyclic extension L_5 of K. The polynomial $g_{s_1}^1(X)$ is investigated to construct certain parametric systems of fundamental units in cyclic quintic fields (cf. [Kih01], [LPS03], [Sch06]).

In the case of char $k=2$, the polynomials $f_{A,B}^{C_5}(X)$ and $h_{A,B}^{C_5}(X)$ are not k-generic for C_5 because $k(x,y)^{D_5}=k(s,t)=k(s,t)(d)$. Hence we should choose another generator of the field $k(x,y)^{C_5}$ over $k(x,y)^{D_5}=k(s,t)$. We take an S_5-primitive C_5-invariant

$$\begin{aligned}e'&:=\sum_{i=0}^{4}\sigma^i(xy^2)\\ &=xy^2+\frac{y(y+1)^2}{x^2}+\frac{(y+1)(x+y+1)^2}{x^3y^2}+\frac{x^2(x+1)}{y}+\frac{(x+1)^2(x+y+1)}{xy^3}\\ &=\frac{x^2+x^3+x^4+x^5+y+x^4y+y^2+x^2y^2+x^5y^2+x^6y^2+y^3+y^4+xy^4+x^4y^5+xy^6}{x^3y^3};\end{aligned}$$

then we have $k(x,y)^{C_5}=k(s,t)(e')$ and the equality

$$e'^2+(s+t+st)e'+1+s+s^3+t^2+t^4+t^5=0.$$

Thus we put

$$\begin{aligned} e &:= \frac{e'}{s+t+st} \\ &= \frac{x^2+x^3+x^4+x^5+y+x^4y+y^2+x^2y^2+x^5y^2+x^6y^2+y^3+y^4+xy^4+x^4y^5+xy^6}{x+x^5+y+x^6y+x^5y^2+x^6y^2+x^5y^4+y^5+x^2y^5+x^4y^5+xy^6+x^2y^6}, \end{aligned}$$

and get $k(x,y)^{C_5} = k(s,t)(e)$; the element e satisfies the following equality of the Artin-Schreier type:

$$e^2 + e + \frac{1+s+s^3+t^2+t^4+t^5}{(s+t+st)^2} = 0. \tag{15}$$

We note that the actions of ρ and $\tau = \rho^2$ on $k(x,y)^{C_5} = k(s,t,e)$ are given by

$$\begin{aligned} \rho \ &: \ s \longmapsto \frac{s+t}{t^2}, \quad t \longmapsto \frac{1}{t}, \quad e \longmapsto e + \frac{1+s+t^2+t^3}{s+t+st}, \\ \tau \ &: \ s \longmapsto s, \quad t \longmapsto t, \quad e \longmapsto e+1. \end{aligned}$$

For an arbitrary field k, by using the action of ρ on $k(s,t)$, a k-generic polynomial for F_{20} is also obtained as follows. The fixed field $k(x,y)^{F_{20}}$ is generated by two elements $\{p,q\}$ over k where

$$p := t - \frac{1}{t}, \quad q := s + \frac{s+5t}{t^2}. \tag{16}$$

Hence the fixed field $k(x,y)^{F_{20}} = k(p,q)$ is purely transcendental over k. The element $(x-1)/x^2$ is an F_{20}-primitive $\langle\rho\rangle$-invariant, and we see

$$\begin{aligned} &\Big\{\pi\Big(\frac{x-1}{x^2}\Big) \ \Big| \ \overline{\pi} \in F_{20}/\langle\rho\rangle\Big\} \\ &= \Big\{\frac{x-1}{x^2}, \frac{y-1}{y^2}, -\frac{x(x+y-1)}{(y-1)^2}, -\frac{xy(x-1)(y-1)}{(x+y-1)^2}, -\frac{y(x+y-1)}{(x-1)^2}\Big\}. \end{aligned}$$

Then we obtain the F_{20}-relative $\langle\rho\rangle$-invariant resolvent polynomial by $(x-1)/x^2$ as

$$\begin{aligned} f_{p,q}^{F_{20}}(X) &:= \mathcal{RP}_{(x-1)/x^2, F_{20}}(X) \\ &= X^5 + \Big(\frac{q^2+5pq-25}{p^2+4} - 2p + 2\Big)X^4 \\ &\quad + \big(p^2 - p - 3q + 5\big)X^3 + (q-3p+8)X^2 + (p-6)X + 1 \ \in \ k(p,q)[X] \end{aligned}$$

for an arbitrary field k, therefore, the polynomial $f_{p,q}^{F_{20}}(X)$ is k-generic for F_{20}.

When char $k \neq 2$, let us put

$$r := -\frac{5p+2q}{2(p^2+4)}.$$

Then from $q = -(5p+8r+2p^2r)/2$ we have $k(p,q) = k(p,r)$. Hence we obtain the following k-generic polynomial $h_{p,r}^{F_{20}}(X) \in k(p,r)[X]$ for F_{20}:

$$\begin{aligned} g_{p,r}^{F_{20}}(X) &:= f_{p,-(5p+8r+2p^2r)/2}^{F_{20}}(X) \\ &= X^5 + \Big(r^2(p^2+4) - 2p - \frac{17}{4}\Big)X^4 + \Big((p^2+4)(3r+1) + \frac{13p}{2} + 1\Big)X^3 \\ &\quad - \Big(r(p^2+4) + \frac{11p}{2} - 8\Big)X^2 + (p-6)X + 1. \end{aligned}$$

The polynomial $g_{p,r}^{F_{20}}(X)$ was constructed by Lecacheux [Lec98].

7. Field intersection problems for solvable quintics

The aim of this section is to give an answer to the field intersection problem of k-generic polynomials $h_{A,B}^{C_5}(X), f_{s,t}^{D_5}(X), f_{p,q}^{F_{20}}(X)$ (or $g_{p,r}^{F_{20}}(X)$ when char $k \neq 2$) explicitly via the relative (multi-) resolvent polynomials.

Let $f_{v_1,v_2}^H(X) \in k(v_1, v_2)[X]$ be a quintic k-generic polynomial with a solvable Galois group H, i.e. $H \leq F_{20}$. For a fixed polynomial $f_{v_1,v_2}^H(X)$, we write

$$L_{\mathbf{a}} := \mathrm{Spl}_M f_{\mathbf{a}}^H(X) \quad \text{and} \quad G_{\mathbf{a}} := \mathrm{Gal}(f_{\mathbf{a}}^H/M)$$

for $\mathbf{a} = (a_1, a_2) \in M^2$. Assume that $G_{\mathbf{a}} \neq \{1\}$. We take the cross-ratios

$$\begin{aligned} x &:= \xi(x_1, \ldots, x_5) = \left(\frac{x_1 - x_4}{x_1 - x_3}\right) \Big/ \left(\frac{x_2 - x_4}{x_2 - x_3}\right), \\ y &:= \eta(x_1, \ldots, x_5) = \left(\frac{x_2 - x_5}{x_2 - x_4}\right) \Big/ \left(\frac{x_3 - x_5}{x_3 - x_4}\right), \end{aligned} \tag{17}$$

and $x' := \xi(y_1, \ldots, y_5)$, $y' := \eta(y_1, \ldots, y_5)$ in the same way as (6) in Section 6. For the two fields $k(\mathbf{x}) = k(x, y)$ and $k(\mathbf{x}') = k(x', y')$, we take the interchanging involution

$$\iota \; : \; k(\mathbf{x}, \mathbf{x}') \longrightarrow k(\mathbf{x}, \mathbf{x}'), \quad (x, y, x', y') \longmapsto (x', y', x, y)$$

which is the special case of $\iota_{\mathbf{x},\mathbf{y}}$ given by (1) in Section 3.

We take elements $\sigma, \tau, \rho, \omega \in \mathrm{Aut}_k(k(x, y))$ as in the previous section; their action on $k(x, y)$ is given by (7). We put $(\sigma', \tau', \rho', \omega') := (\iota^{-1}\sigma\iota, \iota^{-1}\tau\iota, \iota^{-1}\rho\iota, \iota^{-1}\omega\iota) \in \mathrm{Aut}_k(k(x', y'))$ and write

$$\begin{array}{llll} C_5 = \langle \sigma \rangle, & D_5 = \langle \sigma, \tau \rangle, & F_{20} = \langle \sigma, \rho \rangle, & S_5 = \langle \sigma, \omega \rangle, \\ {C_5}' = \langle \sigma' \rangle, & {D_5}' = \langle \sigma', \tau' \rangle, & {F_{20}}' = \langle \sigma', \rho' \rangle, & {S_5}' = \langle \sigma', \omega' \rangle, \\ {C_5}'' = \langle \sigma\sigma' \rangle, & {D_5}'' = \langle \sigma\sigma', \tau\tau' \rangle, & {F_{20}}'' = \langle \sigma\sigma', \rho\rho' \rangle, & {S_5}'' = \langle \sigma\sigma', \omega\omega' \rangle. \end{array}$$

Let Θ be an $S_5 \times {S_5}'$-primitive ${F_{20}}''$-invariant and take the formal $S_5 \times {S_5}'$-relative (resp. $F_{20} \times {F_{20}}'$-relative) ${F_{20}}''$-invariant resolvent polynomial of degree 120 (resp. 20):

$$\begin{aligned} \mathcal{R}_{\mathbf{a},\mathbf{a}'}(X) &:= \mathcal{RP}_{\Theta, S_5 \times {S_5}', f_{\mathbf{a}}^H f_{\mathbf{a}'}^H}(X), \\ \mathcal{R}_{\mathbf{a},\mathbf{a}'}^1(X) &:= \mathcal{RP}_{\Theta, F_{20} \times {F_{20}}', f_{\mathbf{a}}^H f_{\mathbf{a}'}^H}(X). \end{aligned}$$

Since the polynomial $\mathcal{R}_{\mathbf{a},\mathbf{a}'}^1(X)$ divides $\mathcal{R}_{\mathbf{a},\mathbf{a}'}(X)$, we put $\mathcal{R}_{\mathbf{a},\mathbf{a}'}^2(X) := \mathcal{R}_{\mathbf{a},\mathbf{a}'}(X)/\mathcal{R}_{\mathbf{a},\mathbf{a}'}^1(X)$. Note that we need only the polynomial $\mathcal{R}_{\mathbf{a},\mathbf{a}'}^1(X)$ of degree 20 instead of $\mathcal{R}_{\mathbf{a},\mathbf{a}'}(X)$ of degree 120 to treat the intersection problem of $f_{v_1,v_2}^H(X), (H \leq F_{20})$. Indeed we obtain the following theorem:

Theorem 7.1. *For $\mathbf{a} = (a_1, a_2), \mathbf{a}' = (a_1', a_2') \in M^2$, assume that $f_{\mathbf{a}}^H(X)$ and $f_{\mathbf{a}'}^H(X)$ is irreducible over M and $G_{\mathbf{a}} \geq G_{\mathbf{a}'}$. The decomposition type of the polynomial $\mathcal{R}_{\mathbf{a},\mathbf{a}'}^1(X)$ over M and the Galois group $\mathrm{Gal}(\mathcal{R}_{\mathbf{a},\mathbf{a}'}^1/M)$ give an answer to the field intersection problem of $f_{v_1,v_2}^H(X)$ as Table 1 shows. Moreover if $\mathcal{R}_{\mathbf{a},\mathbf{a}'}^1(X)$ has no repeated factors then two splitting fields of $f_{\mathbf{a}}^H(X)$ and of $f_{\mathbf{a}'}^H(X)$ over M coincide if and only if the polynomial $\mathcal{R}_{\mathbf{a},\mathbf{a}'}^1(X)$ has a linear factor over M.*

Table 1

$G_{\mathbf{a}}$	$G_{\mathbf{a}'}$		GAP ID	$G_{\mathbf{a},\mathbf{a}'}$		$\mathrm{DT}(\mathcal{R}^1_{\mathbf{a},\mathbf{a}'})$	$\mathrm{DT}(\mathcal{R}^2_{\mathbf{a},\mathbf{a}'})$
F_{20}	F_{20}	(I-1)	$[400, 205]$	$F_{20} \times F_{20}$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	20	100
		(I-2)	$[200, 42]$	$(D_5 \times D_5) \rtimes C_2$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 2$	10^2	50^2
		(I-3)	$[100, 11]$	$(C_5 \times C_5) \rtimes C_4$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 4$	5^4	50^2
		(I-4)	$[100, 12]$	$(C_5 \times C_5) \rtimes C_4$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 4$	10^2	25^4
		(I-5)	$[20, 3]$	F_{20}	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5^3, 4, 1$	$20^4, 10^2$
	D_5	(I-6)	$[200, 41]$	$F_{20} \times D_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	20	100
		(I-7)	$[100, 10]$	$(C_5 \times C_5) \rtimes C_4$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 2$	20	100
	C_5	(I-8)	$[100, 9]$	$F_{20} \times C_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	20	100
D_5	D_5	(II-1)	$[100, 13]$	$D_5 \times D_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10^2	50^2
		(II-2)	$[50, 4]$	$(C_5 \times C_5) \rtimes C_2$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 2$	5^4	25^4
		(II-3)	$[10, 1]$	D_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5^3, 2^2, 1$	$10^8, 5^4$
	C_5	(II-4)	$[50, 3]$	$D_5 \times C_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10^2	50^2
C_5	C_5	(III-1)	$[25, 2]$	$C_5 \times C_5$	$L_{\mathbf{a}} \neq L_{\mathbf{a}'}$	5^4	25^4
		(III-2)	$[5, 1]$	C_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5^3, 1^5$	5^{20}

We checked the decomposition types on Table 1 using the computer algebra system GAP [GAP].

It seems, however, complicated to compute the resolvent polynomial $\mathcal{R}^1_{\mathbf{a},\mathbf{a}'}(X)$ to display it as an explicit formula. This depends on a choice of an $S_5 \times S_5'$-primitive F_{20}''-invariant Θ and of a minimal basis of the fixed field $K(x, y, x', y')^{F_{20} \times F_{20}'}$ over K. In Subsections 7.1 and 7.2, we first study the reducible and some tractable cases of char $k \neq 2$ and of char $k = 2$, respectively. We treat in Subsection 7.3 the dihedral case and we also evaluate the resolvent polynomial $\mathcal{RP}_{P,D_5''}(X)$ for a certain suitable $D_5 \times D_5'$-primitive D_5''-invariant P explicitly. This case includes also the cyclic case. In Subsection 7.4, we give some numerical examples of Hashimoto-Tsunogai's cyclic quintic and Lehmer's simplest quintic. Finally in Subsection 7.5 we give an answer to the field intersection problem in the case of F_{20}. We do not need to make a formula of another resolvent polynomial because we can use the resolvent $\mathcal{RP}_{P,D_5''}(X)$ given in the dihedral case. We note that the solution of each case is obtained as certain conditions within the base field M.

7.1. **Reducible and tractable cases of char $k \neq 2$.** Throughout this subsection, we assume that char $k \neq 2$. Let $f^H_{v_1,v_2}(X) \in k(v_1, v_2)[X]$ be a k-generic polynomial for H. For the fixed $f^H_{v_1,v_2}(X)$, we write $L_{\mathbf{a}} := \mathrm{Spl}_M f^H_{\mathbf{a}}(X)$ and $G_{\mathbf{a}} := \mathrm{Gal}(f^H_{\mathbf{a}}/M)$ for $\mathbf{a} = (a_1, a_2) \in M^2$. We always assume that $f^H_{\mathbf{a}}(X)$ has no repeated factors over M and $G_{\mathbf{a}} \neq \{1\}$. In this subsection, we treat the case where $f^H_{\mathbf{a}}(X)$ is reducible over M. First we take Brumer's quintic,

$$f^{D_5}_{s,t}(X) = X^5 + (t-3)X^4 + (s-t+3)X^3 + (t^2-t-2s-1)X^2 + sX + t \ \in \ k(s,t)[X].$$

Note that if $f^{D_5}_{s_1,t_1}(X)$ splits over M for $(s_1, t_1) \in M^2$ then the decomposition type $\mathrm{DT}(f^{D_5}_{s_1,t_1})$ over M has to be $2, 2, 1$, and $G_{s_1,t_1} \cong C_2$. We put

$$\delta_{s,t} := s^2 - 4s^3 + 4t - 14st - 30s^2t - 91t^2 - 34st^2 + s^2t^2 + 40t^3 + 24st^3 + 4t^4 - 4t^5$$

as in (9). Then we have

Lemma 7.2. *We take the k-generic polynomial $f^{D_5}_{s,t}(X)$ and suppose* char $k \neq 2$.
(1) *For $(s_1, t_1) \in M^2$, there exists $d_1 \in M$ such that $d_1^2 = \delta_{s_1,t_1}$ if and only if $G_{s_1,t_1} \leq C_5$.*
(2) *In the case of $G_{s_1,t_1} \not\leq C_5$ for $(s_1, s_2) \in M^2$, the quadratic subextension of L_{s_1,s_2} over M is given by $M(\sqrt{\delta_{s_1,t_1}})$.*

Note that in the case of $\mathrm{Gal}(f^{D_5}_{s_1,t_1}/M) \leq C_5$, we convert $f^{D_5}_{s_1,t_1}(X)$ into the Hashimoto-Tsunogai form $f^{C_5}_{A,B}(X)$ or $h^{C_5}_{A,B}(X)$ as in Section 6, (12).

We take a k-generic polynomial for F_{20},

$$g_{p,r}^{F_{20}}(X) = X^5 + \Big(r^2(p^2+4) - 2p - \frac{17}{4}\Big)X^4 + \Big((p^2+4)(3r+1) + \frac{13p}{2} + 1\Big)X^3 \\ -\Big(r(p^2+4) + \frac{11p}{2} - 8\Big)X^2 + (p-6)X + 1 \in k(p,q)[X].$$

Note that, if necessary, we may convert a k-generic polynomial $g_{p,r}^{F_{20}}(X)$ to another form $f_{p,q}^{F_{20}}(X)$ by putting

$$q := -\frac{5p+8r+2p^2r}{2}, \quad \Big(r = -\frac{5p+2q}{2(p^2+4)}\Big).$$

For $(p_1,r_1) \in M^2$, if the polynomial $g_{p_1,r_1}^{F_{20}}(X)$ is reducible over M, the decomposition type $\mathrm{DT}(g_{p_1,r_1}^{F_{20}})$ over M is $4,1$ or $2,2,1$, and $G_{p_1,r_1} \leq C_4$. It follows from (16) that

$$s = \frac{-1}{4}\Big(5p + 8r + 2p^2r + (2pr+5)\sqrt{p^2+4}\Big), \quad t = \frac{1}{2}\Big(p + \sqrt{p^2+4}\Big).$$

Hence the quadratic subextension of $\mathrm{Spl}_{k(p,r)} g_{p,r}^{F_{20}}(X)$ over $k(p,r)$ is $k(p,r)(\sqrt{p^2+4})$.

Lemma 7.3. *We take the k-generic polynomial $g_{p,r}^{F_{20}}(X)$ and suppose* char $k \neq 2$.
(1) *For $(p_1,r_1) \in M^2$, there exists $b \in M$ such that $b^2 = p_1^2+4$ if and only if $G_{p_1,r_1} \leq D_5$. Moreover, in this case of $G_{p_1,r_1} \leq D_5$, the splitting fields of $g_{p_1,r_1}^{F_{20}}(X)$ and of $f_{s_1,t_1}^{D_5}(X)$ over M coincide where $s_1 = -(5p_1 + 8r_1 + 2p_1^2 r_1 + (2p_1r_1+5)b)/4$, $t_1 = (p_1+b)/2$;*
(2) *In the case of $G_{p_1,r_1} \not\leq D_5$, that is, $G_{p_1,r_1} = F_{20}$ or C_4, the quadratic subextension of L_{p_1,r_1} over M is $M(\sqrt{p_1^2+4})$ for $(p_1,r_1) \in M^2$.*

By Lemmas 7.2 and 7.3, we may obtain the subquadratic fields of the splitting fields of polynomials $f_{s_1,t_1}^{D_5}(X)$ and $g_{p_1,r_1}^{F_{20}}(X)$ over M for $s_1,t_1,p_1,r_1 \in M$. For $g_{p_1,r_1}^{F_{20}}(X)$, $(p_1,r_1) \in M^2$, we also get the quartic subfield of L_{p_1,r_1} when $G_{p_1,r_1} \not\leq D_5$. By (9) and (16), we obtain the quartic equation in d:

$$16d^4 - 4(p^2+1)(p^2+4)Wd^2 + (p^2+4)W^2 = 0$$

where

$$W = W_{p,r} := -199 - 16p - 4(19p+41)r + 4(p^2+4)r^2 + 16(p^2+4)r^3. \tag{18}$$

The quartic polynomial

$$g_{p,r}^{C_4}(X) := X^4 - (p^2+1)(p^2+4)WX^2 + (p^2+4)W^2 \in k(p,q)[X] \tag{19}$$

gives the C_4-extension $k(p,q,d) = k(x,y)^{C_5} = k(A,B)$ of $k(p,q)$; by Kemper's theorem [Kem01], this quartic polynomial is k-generic for C_4. We also see

$$d^2 = \delta'_{p,r} := W_{p,r}\Big((p^4+5p^2+4) + p(p^2+3)\sqrt{p^2+4}\Big)\Big/8.$$

Lemma 7.4. *We take the k-generic polynomial $g_{p,r}^{F_{20}}(X)$ and suppose* char $k \neq 2$.
(1) *If $G_{p_1,r_1} = F_{20}$ for $(p_1,r_1) \in M^2$, then the cyclic quartic subfield of $\mathrm{Spl}_M g_{p,r}^{F_{20}}(X)$ over M is given by $M(d_1)$ where d_1 is a square root of δ'_{p_1,r_1};*
(2) *For $(p_1,r_1) \in M^2$, we assume that there exists $b \in M$ such that $b^2 = p_1^2+4$, that is, $G_{p_1,r_1} \leq D_5$. Then there exists $d_1 \in M$ such that $d_1^2 = W_{p_1,r_1}\big((p_1^4+5p_1^2+4) + p_1(p_1^2+3)b\big)/8$ if and only if $G_{p_1,r_1} \leq C_5$.*

In the case where $\mathrm{Gal}(g_{p_1,r_1}^{F_{20}}/M), \mathrm{Gal}(g_{p_1',r_1'}^{F_{20}}/M) \not\leq D_5$, that is, $G_{\mathbf{a}}, G'_{\mathbf{a}} = F_{20}$ or C_4, we should know the coincidence of the cyclic quartic subfields of L_{p_1,r_1} and of $L_{p_1',r_1'}$ over M. In [HM-2], we study the field intersection problem of quartic generic polynomials; an answer to the field isomorphism problem of k-generic polynomial for C_4 is given as follows. First, the following lemma is well-known (cf. [JLY02, Chapter 2]):

Lemma 7.5. *Assume* char $k \neq 2$.
(1) *The polynomial* $f_{s,t}^{D_4}(X) = X^4 + sX^2 + t \in k(s,t)[X]$ *is* k*-generic for* D_4*;*
(2) *For* $(a,b) \in M^2$, $\mathrm{Gal}(f_{a,b}^{D_4}/M) \leq C_4$ *if and only if there exists* $c \in M$ *such that* $c^2 = (a^2 - 4b)/b$.

From Lemma 7.5, we see that the polynomial

$$f_{s,u}^{C_4}(X) := X^4 + sX^2 + \frac{s^2}{u^2+4} \in k(s,u)[X]$$

is k-generic for C_4. The discriminant of $f_{s,u}^{C_4}(X)$ with respect to X equals $16\, s^6 u^4/(u^2+4)^3$. By using the polynomial $f_{s,u}^{C_4}(X)$ above, we get the following theorem:

Theorem 7.6 ([HM-2])**.** *We suppose* char $k \neq 2$ *and take the* k*-generic polynomial* $f_{s,u}^{C_4}(X) := X^4 + sX^2 + s^2/(u^2+4) \in k(s,u)[X]$ *for* C_4*. For* $\mathbf{a} = (a,c)$, $\mathbf{a}' = (a',c') \in M^2$ *with* $aa'cc'(c^2+4)(c'^2+4) \neq 0$, *we assume that* $c \neq \pm c'$ *and* $c \neq \pm 4/c'$. *Then the splitting fields of* $f_{a,c}^{C_4}(X)$ *and of* $f_{a',c'}^{C_4}(X)$ *over* M *coincide if and only if the polynomial* $F_{\mathbf{a},\mathbf{a}'}(X) = F_{\mathbf{a},\mathbf{a}'}^{+}(X) F_{\mathbf{a},\mathbf{a}'}^{-}(X)$ *has a linear factor over* M *where*

$$F_{\mathbf{a},\mathbf{a}'}^{\pm}(X) = X^4 - aa'X^2 + \frac{a^2 a'^2 (c \pm c')^2}{(c^2+4)(c'^2+4)}.$$

Remark 7.7. We note that the polynomial $F_{\mathbf{a},\mathbf{a}'}(X)$ in Theorem 7.6 is obtained as the resolvent polynomial $\mathcal{RP}_{\Theta,D_4,f}(X)$ for a certain $D_4 \times D_4'$-primitive D_4''-invariant with $f(X) = f_{\mathbf{a}}^{D_4}(X) f_{\mathbf{a}'}^{D_4}(X)$. The discriminant of $F_{\mathbf{a},\mathbf{a}'}^{\pm}(X)$ is given by $16 a^6 a'^6 (c \pm c')^2 (cc' \mp 4)^4/((c^2+4)^3(c'^2+4)^3)$. Hence the condition $aa' \neq 0$, $c \neq \pm c'$ and $c \neq \pm 4/c'$ implies that $F_{\mathbf{a},\mathbf{a}'}(X)$ has no repeated factors. We may assume that the condition $aa' \neq 0$, $c \neq \pm c'$ and $c \neq \pm 4/c'$ without loss of generality as in Remark 2.3 (see also [HM-2]).

Applying Theorem 7.6 to the polynomial $g_{p,r}^{C_4}(X)$ as in (19), in the case of

$$a = -(p^2+1)(p^2+4)W, \quad b = (p^2+4)W^2, \quad c = p(p^2+3),$$

we obtain a criterion in terms of the condition within the field M to determine whether the sub-quartic fields of the splitting fields of $g_{p_1,r_1}^{F_{20}}(X)$ and of $g_{p_1',r_1'}^{F_{20}}(X)$ coincide or not.

Remark 7.8. In the case where the field M includes a primitive 4th root $i := e^{2\pi\sqrt{-1}/4}$ of unity, by Kummer theory, the polynomial $h_t^{C_4}(X) := X^4 - t \in k(t)[X]$ is k-generic for C_4. Indeed we see that the polynomials $f_{a,c}^{C_4}(X) = X^4 + aX^2 + a^2/(c^2+4)$ and $X^4 - a^2(c-2i)/(c+2i)$ are Tschirnhausen equivalent over M because

$$\mathrm{Resultant}_X\Big(f_{a,c}^{C_4}(X), Y - \Big(\frac{(c+i)(c-2i)}{c}X + \frac{c^2+4}{ac}X^3\Big)\Big) = Y^4 - \frac{a^2(c-2i)}{c+2i}.$$

In this case, for $b, b' \in M$ with $b \cdot b' \neq 0$, the splitting fields of $h_b^{C_4}(X)$ and of $h_{b'}^{C_4}(X)$ over M coincide if and only if the polynomial $(X^4 - bb')(X^4 - b^3 b')$ has a linear factor over M.

7.2. **Reducible and tractable cases of char** $k = 2$**.** Throughout this subsection we assume that char $k = 2$. As in the previous subsection, we treat the reducible and the tractable cases for a field k of char $k = 2$.

We first note that, by Artin-Schreier theory, the polynomial $f_t^{C_2}(X) := X^2 + X + t \in k(t)$ is k-generic for C_2. We take the k-generic polynomial

$$f_{s,t}^{D_5}(X) = X^5 + (t+1)X^4 + (s+t+1)X^3 + (t^2+t+1)X^2 + sX + t$$

of the Brumer's form for D_5 where $k(x,y)^{D_5} = k(s,t)$. We denote the constant term of the equation (15) by

$$\epsilon_{s,t} := \frac{1+s+s^3+t^2+t^4+t^5}{(s+t+st)^2}.$$

Then we have

Lemma 7.9. *Assume char $k=2$. For the k-generic polynomial $f_{s,t}^{D_5}(X)$, the following two assertions hold*:
(1) *For $(s_1,t_1)\in M^2$, there exists $e_1\in M$ such that $e_1^2=e_1+\epsilon_{s_1,t_1}$ if and only if $G_{s_1,t_1}\leq C_5$;*
(2) *In the case of $G_{s_1,t_1}\not\leq C_5$ for $(s_1,s_2)\in M^2$, the quadratic subextension of L_{s_1,s_2} over M is given as the splitting field of $X^2+X+\epsilon_{s_1,t_1}$ over M.*

For the Frobenius group F_{20} of order 20, we take the k-generic polynomial

$$f_{p,q}^{F_{20}}(X)=X^5+\Big(\frac{q^2+pq+1}{p^2}\Big)X^4+(p^2+p+q+1)X^3+(p+q)X^2+pX+1$$

as in the previous section, where $k(x,y)^{F_{20}}=k(p,q)$. From (16), we get the relations,

$$t^2+pt+1=0,\quad ps+qt+1=0. \tag{20}$$

It follows from

$$s=(qt+1)/p \tag{21}$$

that $k(x,y)^{D_5}=k(p,q)(t)$. We put

$$T:=t/p \tag{22}$$

and have $T^2+T+1/p^2=0$. Hence the quadratic subfield $k(p,q)(T)$ of $\mathrm{Spl}_{k(p,q)}f_{p,q}^{F_{20}}(X)$ over $k(p,q)$ is given as the splitting field of the polynomial

$$X^2+X+1/p^2$$

of the Artin-Schreier type over $k(p,q)$.

Lemma 7.10. *Assume* char $k=2$. *For the k-generic polynomial $f_{p,q}^{F_{20}}(X)$, the following two assertions hold*:
(1) *For $(p_1,q_1)\in M^2$, there exists $b\in M$ such that $b^2=b+1/p_1^2$ if and only if $G_{p_1,q_1}\leq D_5$;*
(2) *In the case of $G_{p_1,q_1}\not\leq D_5$, that is, $G_{p_1,q_1}=F_{20}$ or C_4, the quadratic subextension of L_{p_1,q_1} over M is given as the splitting field of X^2+X+1/p_1^2 over M for $(p_1,q_1)\in M^2$.*

From Lemmas 7.9 and 7.10, we obtain the subquadratic fields of the splitting fields of polynomials $f_{s_1,t_1}^{D_5}(X)$ and $f_{p_1,q_1}^{F_{20}}(X)$ over M for $s_1,t_1,p_1,q_1\in M$. We are able to distinguish such quadratic fields by the following well-known lemma (cf. [AS26]):

Lemma 7.11 (Artin-Schreier [AS26])**.** *Take the k-generic polynomial $f_s^{C_2}(X)=X^2+X+s$ for C_2. For $a,a'\in M,(a,a'\notin\{c^2+c\,|\,c\in M\})$, the splitting fields of $f_a^{C_2}(X)$ and of $f_{a'}^{C_2}(X)$ over M coincide if and only if the polynomial $f_{a+a'}^{C_2}(X)=X^2+X+(a+a')$ has a linear factor over M.*

Next, we consider when the quartic subfields of $\mathrm{Spl}_M f_{p_1,p_2}^{F_{20}}(X)$ and of $\mathrm{Spl}_M f_{p_1',p_2'}^{F_{20}}(X)$ coincide for $(p_1,q_1),(p_1',q_1')\in M^2$ under the condition $G_{p_1,q_1},G_{p_1',q_1'}\not\leq D_5$. By Lemma 7.11, we should treat only the case where the splitting fields of X^2+X+1/p_1^2 and of $X^2+X+1/p_1'^2$ over M coincide. In this case, we may also assume that $p_1=p_1'=:P_1$ because two polynomials X^2+X+1/p_1^2 and $X^2+X+1/p_1'^2$ are Tschirnhausen equivalent over M.

We may use the following classical lemma ([Alb34]):

Lemma 7.12 (Albert [Alb34], Theorems 4 and 19)**.** *Let $M(x)$ and $M(y)$ be cyclic quartic fields over M with a common quadratic subfield $M(u)$ over M so that we may assume*

$$u^2=u+a,\quad x^2=x+(au+b),\quad y^2=y+(au+b)+c$$

for some $a,b,c\in M$ with $a\notin\{d^2+d\,|\,d\in M\}$. Then the fields $M(x)$ and $M(y)$ coincide if and only if the polynomial $X^2+X+(a+c)$ has a linear factor over M.

By the equalities (15), (20), (21) and (22), we see that $k(x,y)^{F_{20}} = k(p,q)$, $k(x,y)^{D_5} = k(p,q)(T)$ and $k(x,y)^{C_5} = k(p,q)(T,e) = k(p,q)(e)$, where

$$\begin{aligned}
&T^2+T+1/p^2=0,\\
&e^2+e+\frac{1+p^3+p^5+pq+p^3q+q^2}{p(1+q)^2}T+\frac{p^4+p^5+p^6+q+p^4q+pq^2+q^3}{p^2(1+q)^2}=0.
\end{aligned}$$

In order to apply Lemma 7.12 to the cyclic quartic extension $k(p,q)(e)/k(p,q)$, we modify the primitive element e by putting

$$E := e+\frac{1+p+q+p^3}{p(1+q)}(T+1)+\frac{1+q+p^2}{p^2(1+q)}. \tag{23}$$

Then we have $k(x,y)^{C_5} = k(p,q)(E)$, $k(x,y)^{D_5} = k(p,q)(T)$ and the equalities

$$\begin{aligned}
&T^2+T+\frac{1}{p^2}=0,\\
&E^2+E+\frac{T}{p^2}+\frac{1+p+p^4+p^5+q+q^3}{p^2(1+q)^2}=0.
\end{aligned}$$

Hence we may apply Lemma 7.12 to our situation where

$$u=T,\ a=\frac{1}{P_1^2},\ b=\frac{1+P_1+P_1^4+P_1^5+q_1+q_1^3}{P_1^2(1+q_1)^2},\ c=b+\frac{1+P_1+P_1^4+P_1^5+q_1'+q_1'^3}{P_1^2(1+q_1')^2}$$

and $P_1 := p_1 = p_1'$. In particular, we obtain a criterion whether the subquartic fields of the splitting fields of $f^{F_{20}}_{p_1,r_1}(X)$ and of $f^{F_{20}}_{p_1',r_1'}(X)$ coincide or not, in terms of the condition within the field M.

By the result of Subsections 7.1 and 7.2, we reach a partial solution of the field intersection problem of $f^{D_5}_{s,t}(X)$ and $f^{F_{20}}_{p,q}(X)$ (or $g^{F_{20}}_{p,r}(X)$ when char $k \neq 2$) in the reducible cases, that is, $G_{\mathbf{a}} \le C_4$, and also in the case where two splitting fields $L_{\mathbf{a}}$ and $L_{\mathbf{a}'}$ have either a quadratic or a quartic subfield over M as the intersection. Namely we determined the situation except for the cases {(I-3),(I-4),(I-5)},{(II-2),(II-3)},{(III-1),(III-2)} on Table 1.

7.3. **Dihedral case.** Let k be an arbitrary field. In this subsection we investigate the method to distinguish the difference of the cases {(II-2),(II-3)} and {(III-1),(III-2)} on Table 1. We use the k-generic polynomial

$$f^{D_5}_{s,t}(X) = X^5+(t-3)X^4+(s-t+3)X^3+(t^2-t-2s-1)X^2+sX+t$$

for D_5. Note that $k(\mathbf{s}) := k(s,t) = k(x,y)^{D_5}$ where s and t are given in terms of x,y by

$$\begin{aligned}
s&=-(x-2x^2+x^3+y-4xy+5x^2y-3x^3y+x^4y-2y^2+5xy^2\\
&\qquad -5x^2y^2+2x^3y^2+y^3-3xy^3+2x^2y^3-x^3y^3+xy^4)/(x^2y^2),\\
t&=-\frac{(x-1)(y-1)(x+y-1)}{xy}
\end{aligned}$$

as in (8). We set $(s',t',d') := \iota(s,t,d)$ and $\mathbf{s}' = (s',t')$. In the case of $f^{D_5}_{s,t}(X)$, we take

$$\begin{aligned}
P &:= \sum_{i=0}^{4}(\sigma\sigma')^i(xx')\\
&= xx'+yy'+\frac{(y-1)(y'-1)}{xx'}+\frac{(x+y-1)(x'+y'-1)}{xx'yy'}+\frac{(x-1)(x'-1)}{yy'}
\end{aligned}$$

as a suitable $D_5 \times D_5'$-primitive D_5''-invariant.

To distinguish the cases (II-2) and (II-3), we evaluate the formal $D_5 \times D_5'$-relative D_5''-invariant resolvent polynomial by P. In the case of char $k \neq 2$, the result is given as follows:

$$\begin{aligned} F^1_{\mathbf{s},\mathbf{s}'}(X) &:= \mathcal{RP}_{P,D_5\times D_5'}(X) = \prod_{\overline{\pi}\in(D_5\times D_5')/D_5''}(X-\pi(P)) \\ &= \Big(G^1_{\mathbf{s},\mathbf{s}'}(X)\Big)^2 - \frac{d^2d'^2}{4}\Big(G^2_{\mathbf{s},\mathbf{s}'}(X)\Big)^2 \ \in k(s,t,s',t')[X] \end{aligned}$$

where

$$\begin{aligned} G^1_{\mathbf{s},\mathbf{s}'}(X) &= X^5-(t-3)(t'-3)X^4+c_3X^3+\frac{c_2}{2}X^2+\frac{c_1}{2}X+\frac{c_0}{2}, \\ G^2_{\mathbf{s},\mathbf{s}'}(X) &= X^2+(t+t'-1)X+s-t+s'-t'+tt'+2 \end{aligned} \tag{24}$$

and $c_3, c_2, c_1, c_0 \in k(s,t,s',t')$ are given by

$$\begin{aligned} c_3 &= \big[2s-21t+3t^2-2ts'+t^2s'-t^2t'\big]+31-3ss'+5tt', \\ c_2 &= \big[-20s+112t+8st-32t^2+2t^3+5ts'-13sts'-12t^2s'+4t^3s'-15stt' \\ &\quad +14t^2t'+2t^3t'+8t^2s't'-2t^3t'^2\big]-102+27ss'-119tt'-sts't'+6t^2t'^2, \\ c_1 &= \big[32s+2s^2-128t-26st+60t^2+4st^2-8t^3-6s^2s'-7ts'+38sts'+9t^2s'-5st^2s' \\ &\quad -12t^3s'+2t^4s'-20ts'^2-8sts'^2+6t^2s'^2+2t^3s'^2+2stt'-77t^2t'+3st^2t'+8t^3t'-29t^2s't' \\ &\quad +st^2s't'+18t^3s't'-2st^2t'^2+10t^3t'^2\big]+80-37ss'+145tt'-45sts't'+24t^2t'^2-8t^3t'^3, \\ c_0 &= \big[-16s-2s^2+56t+24st+2s^2t-38t^2-8st^2+8t^3+5s^2s'-2ts'-38sts'-7s^2ts' \\ &\quad +5t^2s'+13st^2s'+8t^3s'+2st^3s'-4t^4s'-21ts'^2-11sts'^2-2t^2s'^2+2st^2s'^2+4t^3s'^2 \\ &\quad -104stt'-33s^2tt'+105t^2t'+35st^2t'+4t^3t'+16st^3t'-6t^4t'-2t^5t'-s^2ts't'+36t^2s't' \\ &\quad -14st^2s't'-6t^3s't'+6t^4s't'+8t^2s'^2t'-37st^2t'^2+22t^3t'^2-2st^3t'^2+8t^4t'^2+8t^3s't'^2 \\ &\quad -2t^4t'^3\big]-24+14ss'-8s^2s'^2-224tt'+sts't'-101t^2t'^2-st^2s't'^2-8t^3t'^3 \end{aligned}$$

with simplifying notation $\big[a\big] := a+\iota(a)$ for $a \in k(s,t,s',t')$. It follows from the definition of ι that $\iota(s,t,s',t') = (s',t',s,t)$. We also note that $d^2 = \delta_{s,t} \in k(s,t)$ and $d'^2 = \delta_{s',t'} \in k(s',t')$ where δ is given by the formula (9).

In the case of char $k = 2$, the result is

$$F^1_{\mathbf{s},\mathbf{s}'}(X) = \Big(G^3_{\mathbf{s},\mathbf{s}'}(X)\Big)^2 + G^3_{\mathbf{s},\mathbf{s}'}(X)\cdot G^4_{\mathbf{s},\mathbf{s}'}(X) + (e^2+e)(e'^2+e')\Big(G^4_{\mathbf{s},\mathbf{s}'}(X)\Big)^2$$

where

$$\begin{aligned} G^3_{\mathbf{s},\mathbf{s}'}(X) &= X^5+(t+1)(t'+1)X^4+d_3X^3+d_2X^2+d_1X+d_0, \\ G^4_{\mathbf{s},\mathbf{s}'}(X) &= (s+t+st)(s'+t'+s't')(X^2+(t+t'+1)X+s+t+s'+t'+tt') \end{aligned}$$

and $d_3, d_2, d_1, d_0 \in k(s,t,s',t')$ are given by

$$\begin{aligned} d_3 &= \big[t(1+t+ts'+tt')\big]+1+ss'+tt', \\ d_2 &= \big[s+t+st+t^3+ts'+sts'+stt'+t^2t'+t^3t'+t^3t'^2\big]+1+ss'+sts't'+t^2t'^2, \\ d_1 &= \big[s+s^2+t+st+t^2+st^2+s^2s'+ts'+sts'+t^2s'+st^2s'+t^4s'+t^2s'^2+t^3s'^2 \\ &\quad +t^2t'+t^3s't'+st^2t'^2+t^3t'^2\big]+tt'(1+ss'), \\ d_0 &= \big[t(st+sts'+st^2s'+ts'^2+sts'^2+t^3t'+t^4t'+s^2s't'+sts't'+t^2s't'+t^3s't' \\ &\quad +t^2t'^2+st^2t'^2+t^3t'^3)\big]+tt'(1+ss')(1+tt') \end{aligned}$$

with simplifying notation $[a] := a + \iota(a)$ for $a \in k(s,t,s',t')$. Note that $e^2 + e = \epsilon_{s,t} \in k(s,t)$ and $e'^2 + e' = \epsilon_{s',t'} \in k(s',t')$ where $\epsilon_{s,t}$ is given above as the constant term in (15).

Note that the polynomial $F^1_{\mathbf{s},\mathbf{s}'}(X)$ splits into two factors over the field $k(s,t,s',t')(d,d')$ (resp. $k(s,t,s',t')(e,e')$) when char $k \neq 2$ (resp. char $k = 2$) as

$$F^1_{\mathbf{s},\mathbf{s}'}(X) = \Big(G^1_{\mathbf{s},\mathbf{s}'}(X) + \frac{dd'}{2}G^2_{\mathbf{s},\mathbf{s}'}(X)\Big)\Big(G^1_{\mathbf{s},\mathbf{s}'}(X) - \frac{dd'}{2}G^2_{\mathbf{s},\mathbf{s}'}(X)\Big),$$
$$F^1_{\mathbf{s},\mathbf{s}'}(X) = \Big(G^3_{\mathbf{s},\mathbf{s}'}(X) + (e+e')G^4_{\mathbf{s},\mathbf{s}'}(X)\Big)\Big(G^3_{\mathbf{s},\mathbf{s}'}(X) + (e+e'+1)G^4_{\mathbf{s},\mathbf{s}'}(X)\Big).$$

From Theorem 7.1 and Table 1, we have to determine when it occurs that $\omega_f(\pi(P)) \in M$ for some $\overline{\pi} \in (F_{20} \times F'_{20})/F''_{20}$ where $f = f^{D_5}_{s_1,t_1} \cdot f^{D_5}_{s'_1,t'_1}$ with $(s_1,t_1),(s'_1,t'_1) \in M^2$. Thus we take an element $\rho(P) \in k(s,t)$ which is conjugate of P under the action of $F_{20} \times F'_{20}$ but not under the action of $D_5 \times D'_5$. We put

$$F^2_{\mathbf{s},\mathbf{s}'}(X) := \mathcal{RP}_{\rho(P),D_5\times D'_5}(X) = F^1_{\rho(s),\rho(t),s',t'}(X) = \rho\big(F^1_{\mathbf{s},\mathbf{s}'}(X)\big)$$

where ρ acts on $k(s,t)$ as in (14). Then the polynomial $F^1_{\mathbf{s},\mathbf{s}'}(X) \cdot F^2_{\mathbf{s},\mathbf{s}'}(X)$ becomes the formal $F_{20} \times D'_5$-relative D''_5-invariant resolvent polynomial by P. We state the result of the dihedral case.

Theorem 7.13. *We take the k-generic polynomial $f^{D_5}_{s,t}(X)$ over an arbitrary field k. For $\mathbf{a} = (a_1,a_2)$, $\mathbf{a}' = (a'_1,a'_2) \in M^2$, we assume that $G_{\mathbf{a}} \geq G_{\mathbf{a}'} \geq C_5$. An answer to the field intersection problem of $f^{D_5}_{s,t}(X)$ is given by* $\mathrm{DT}(F^1_{\mathbf{a},\mathbf{a}'})$ *and* $\mathrm{DT}(F^2_{\mathbf{a},\mathbf{a}'})$ *as Table 2 shows.*

Table 2

$G_{\mathbf{a}}$	$G_{\mathbf{a}'}$		GAP ID	$G_{\mathbf{a},\mathbf{a}'}$		$\mathrm{DT}(F^1_{\mathbf{a},\mathbf{a}'})$	$\mathrm{DT}(F^2_{\mathbf{a},\mathbf{a}'})$
D_5	D_5	(II-1)	$[100,13]$	$D_5 \times D_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
		(II-2)	$[50,4]$	$(C_5 \times C_5) \rtimes C_2$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 2$	5^2	5^2
		(II-3)	$[10,1]$	D_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5,2^2,1$	5^2
						5^2	$5,2^2,1$
	C_5	(II-4)	$[50,3]$	$D_5 \times C_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
C_5	C_5	(III-1)	$[25,2]$	$C_5 \times C_5$	$L_{\mathbf{a}} \neq L_{\mathbf{a}'}$	5^2	5^2
		(III-2)	$[5,1]$	C_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5,1^5$	5^2
						5^2	$5,1^5$

Remark 7.14. In the reducible case, that is, the case of $G_{\mathbf{a}'} = C_2$, we obtain an answer to the subfield problem of $f^{D_5}_{s,t}(X)$ via $\mathrm{DT}(F^i_{\mathbf{a},\mathbf{a}'})$ for $i = 1,2$ as on Table 3 (cf. Lemma 7.2):

Table 3

$G_{\mathbf{a}}$	$G_{\mathbf{a}'}$	GAP ID	$G_{\mathbf{a},\mathbf{a}'}$		$\mathrm{DT}(F^1_{\mathbf{a},\mathbf{a}'})$	$\mathrm{DT}(F^2_{\mathbf{a},\mathbf{a}'})$
D_5	C_2	$[20,4]$	D_{10}	$L_{\mathbf{a}} \not\supset L_{\mathbf{b}}$	10	10
		$[10,1]$	D_5	$L_{\mathbf{a}} \supset L_{\mathbf{b}}$	5^2	5^2
C_5		$[10,2]$	C_{10}	$L_{\mathbf{a}} \cap L_{\mathbf{b}} = M$	10	10
C_2		$[4,2]$	$C_2 \times C_2$	$L_{\mathbf{a}} \neq L_{\mathbf{b}}$	$4^2,2$	$4^2,2$
		$[2,1]$	C_2	$L_{\mathbf{a}} = L_{\mathbf{b}}$	$2^4,1^2$	$2^4,1^2$

Example 7.15. We take $M = \mathbb{Q}$ and write $L_{s_1,t_1} := \mathrm{Spl}_{\mathbb{Q}} f^{D_5}_{s_1,t_1}(X)$ and $G_{s_1,t_1} := \mathrm{Gal}(f^{D_5}_{s_1,t_1}/\mathbb{Q})$ for $(s_1,t_1) \in \mathbb{Q}^2$. As in Example 6.2, for $s_1 \in \mathbb{Q}$, two polynomials

$$f^{D_5}_{s_1,1}(X) = X^5 - 2X^4 + (s_1+2)X^3 - (2s_1+1)X^2 + s_1X + 1,$$
$$f^{D_5}_{s_1+5,-1}(X) = X^5 - 4X^4 + (s_1+9)X^3 - (2s_1+9)X^2 + (s_1+5)X - 1$$

have the same splitting field over $\mathbb{Q}$, i.e. $L_{s_1,1} = L_{s_1+5,-1}$. By Theorem 7.13, we also see $L_{0,1} = L_{-1,1}$ because $F^1_{0,1,-1,1}(X)$ and $F^2_{0,1,-1,1}(X)$ split over $\mathbb{Q}$ into the following irreducible factors:

$$\begin{aligned} F^1_{0,1,-1,1}(X) &= (X^5 - 4X^4 - 3X^3 + 23X^2 + 7X - 25) \\ &\quad \cdot (X^5 - 4X^4 - 3X^3 - 24X^2 - 40X - 25), \\ F^2_{0,1,-1,1}(X) &= X(X^2 - 3X + 14)(X^2 - 5X + 18) \\ &\quad \cdot (X^5 - 8X^4 + 47X^3 - 171X^2 + 299X - 235). \end{aligned}$$

Hence we get $L_{5,-1} = L_{0,1} = L_{-1,1} = L_{4,-1}$ and $G_{5,-1} = G_{0,1} = G_{-1,1} = G_{4,-1} = D_5$. The equalities $L_{5,-1} = L_{0,1}$ and $L_{-1,1} = L_{4,-1}$ can be checked via Theorem 7.13 as

$$\begin{aligned} F^2_{5,-1,0,1}(X) &= X(X+1)^2(X-3)^2(X^5 - 4X^4 - 2X^3 - 35X^2 - 38X - 47), \\ F^2_{-1,1,4,-1}(X) &= X(X-1)^2(X-7)^2(X^5 - 16X^4 + 78X^3 - 159X^2 + 190X - 611). \end{aligned}$$

In these cases, the decomposition types $\mathrm{DT}(F^2_{5,-1,0,1}/\mathbb{Q})$ and $\mathrm{DT}(F^2_{-1,1,4,-1}/\mathbb{Q})$ should be $5, 2^2, 1$ (cf. Theorem 2.1 about multiple factors).

For $s_1, s_1' \in \mathbb{Z}$ with $-10000 \le s_1 < s_1' \le 10000$, we see that $L_{s_1,1} = L_{s_1',1}$ if and only if $(s_1, s_1') \in X_1 \cup X_2$ where

$$\begin{aligned} X_1 &= \{(-6,0), (-1,41), (-94,-10)\}, \\ X_2 &= \{(-1,0), (-6,-1), (-18,-7), (1,34), (0,41), (-6,41), (-167,-8)\}. \end{aligned}$$

It can be checked directly that, for $s_1, s_1' \in \mathbb{Z}$ in the range $-10000 \le s_1 < s_1' \le 10000$ and for each of $i = 1, 2$, $(s_1, s_1') \in X_i$ if and only if the decomposition type $\mathrm{DT}(F^i_{s_1,1,s_1',1}/\mathbb{Q})$ includes 1. Note that if $(s_1, s_1') \in X_1 \cup X_2$ then $G_{s_1,1} = G_{s_1',1} = D_5$ except for $(s_1, s_1') = (-18, -7)$. We see $G_{-18,1} = G_{-7,1} = C_5$ because $\mathrm{DT}(F^2_{18,1,-7,1}/\mathbb{Q})$ is $5, 1^5$ as follows:

$$\begin{aligned} F^2_{18,1,-7,1}(X) &= (X+5)(X-6)^2(X+16)(X-17) \\ &\quad \cdot (X^5 - 8X^4 - 289X^3 + 777X^2 + 7679X - 23671). \end{aligned}$$

Example 7.16. We take $M = \mathbb{Q}$. In [KRY], Kida-Renault-Yokoyama showed that there exist infinitely many $b \in \mathbb{Q}$ such that the polynomials $f^{D_5}_{0,1}(X)$ and $f^{D_5}_{b,1}(X)$ have the same splitting field over $\mathbb{Q}$. Their method enables us to construct such b's explicitly via rational points of the associated elliptic curve (cf. [KRY]). They also pointed out that in the range $-400 \le s_1, t_1 \le 400$ there are 25 pairs $(s_1, t_1) \in \mathbb{Z}^2$ such that the splitting fields of $f^{D_5}_{0,1}(X)$ and of $f^{D_5}_{s_1,t_1}(X)$ over $\mathbb{Q}$ coincide. We may classify the 25 pairs by the polynomials $F^1_{0,1,s_1,t_1}(X)$ and $F^2_{0,1,s_1,t_1}(X)$. For $i = 1, 2$, in the range above, the decomposition type $\mathrm{DT}(F^i_{0,1,s_1,t_1}/\mathbb{Q})$ includes 1 if and only if $(s_1, t_1) \in X_i$ where

$$\begin{aligned} X_1 = \{&(0,1), (4,-1), (4,5), (-6,1), (-24,19), (34,11), (36,-5), \\ &(46,-1), (-188,23), (264,31), (372,-5), (378,43)\}, \\ X_2 = \{&(-1,-1), (-1,1), (5,-1), (41,1), (-43,5), (47,13), (59,-5), \\ &(59,19), (101,19), (125,-23), (149,11), (155,25), (-169,55)\}. \end{aligned}$$

By Theorem 7.13, we see that if $F^1_{0,1,s_1,t_1}(X)$ (resp. $F^2_{0,1,s_1,t_1}(X)$), $(s_1, t_1) \in \mathbb{Z}^2$, has a root in $\mathbb{Q}$ then $(s_1, t_1) = (2u, 2v+1)$ (resp. $(s_1, t_1) = (2u+1, 2v+1)$) for some $u, v \in \mathbb{Z}$ because $F^1_{0,1,s_1,t_1}(X) \in \mathbb{Z}[X]$ splits into irreducible factors over the field $\mathbb{F}_2$ of two elements as

$$\begin{aligned} F^1_{0,1,0,0}(X) &= (X^5 + X^3 + 1)^2, \\ F^1_{0,1,0,1}(X) &= X(X+1)^4(X^5 + X^2 + 1), \\ F^1_{0,1,1,0}(X) &= X^{10} + X^7 + X^4 + X^3 + 1, \\ F^1_{0,1,1,1}(X) &= (X^5 + X^3 + 1)(X^5 + X^3 + X^2 + X + 1) \end{aligned}$$

and $F^2_{0,1,s_1,t_1}(X) \in \mathbb{Z}[X]$ also splits into irreducible factors over $\mathbb{F}_2$ as

$$\begin{aligned}
F^2_{0,1,0,0}(X) &= (X^5+X^3+1)^2,\\
F^2_{0,1,0,1}(X) &= (X^5+X^3+1)(X^5+X^3+X^2+X+1),\\
F^2_{0,1,1,0}(X) &= X^{10}+X^7+X^6+X^4+X^2+X+1,\\
F^2_{0,1,1,1}(X) &= X^3(X+1)^2(X^5+X^3+X^2+X+1).
\end{aligned}$$

We do not know, however, whether there exist infinitely many pairs $(s_1,t_1) \in \mathbb{Z}^2$ such that $\mathrm{Spl}_{\mathbb{Q}} f^{D_5}_{0,1}(X) = \mathrm{Spl}_{\mathbb{Q}} f^{D_5}_{s_1,t_1}(X)$ or not. By Theorem 7.13, we checked such pairs $(s_1,t_1) \in \mathbb{Z}^2$ in the range $-20000 \le s_1, t_1 \le 20000$ and added just $\{(526,41), (952,113), (2302,95), (6466,311), (7180,143), (7480,-169)\}$ to X_1, and $\{(785,-25), (3881,29), (-11215,299), (19739,-281)\}$ to X_2.

7.4. **Cyclic case.** Assume that char $k \ne 2$. We take Hashimoto-Tsunogai's k-generic polynomial

$$h^{C_5}_{A,B}(X) = X^5 - \frac{P}{Q^2}(A^2-2A+15B^2+2)X^3 + \frac{P^2}{Q^3}(2BX^2-(A-1)X-2B) \in k(A,B)[X]$$

for C_5 where $P = (A^2-A-1)^2+25(A^2+1)B^2+125B^4$, $Q = 1-A+7B^2+AB^2$.

The polynomials $h^{C_5}_{A,B}(X)$ and $f^{C_5}_{A,B}(X)$ have the same splitting field over $k(A,B)$, and $f^{C_5}_{A,B}(X)$ is defined by Brumer's form $f^{D_5}_{s,t}(X)$ as in (12). Therefore, we already have a solution for the field isomorphism problem of $f^{C_5}_{A,B}(X)$ and of $h^{C_5}_{A,B}(X)$ from the result of the previous subsection. In this case we see that the formal resolvent polynomials $F^1_{\mathbf{s},\mathbf{s}'}(X)$ and $F^2_{\mathbf{s},\mathbf{s}'}(X)$ split over $k(s,t,s',t')(d,d')$ as

$$F^1_{\mathbf{s},\mathbf{s}'}(X) = H^1_{\mathbf{s},\mathbf{s}'}(X)\cdot H^3_{\mathbf{s},\mathbf{s}'}(X), \quad F^2_{\mathbf{s},\mathbf{s}'}(X) = H^2_{\mathbf{s},\mathbf{s}'}(X)\cdot H^4_{\mathbf{s},\mathbf{s}'}(X)$$

where $H^i_{\mathbf{s},\mathbf{s}'}(X)$, $(1 \le i \le 4)$ is the formal $C_5 \times C_5'$-relative C_5''-resolvent polynomial of degree 5 by $\rho^{i-1}(P)$ and given by

$$\begin{aligned}
H^i_{\mathbf{s},\mathbf{s}'}(X) &:= \mathcal{RP}_{\rho^{i-1}(P),C_5\times C_5'}(X) = \rho^{i-1}\big(\mathcal{RP}_{P,C_5\times C_5'}(X)\big)\\
&= \rho^{i-1}\Big(G^1_{\mathbf{s},\mathbf{s}'}(X) - \frac{dd'}{2}G^2_{\mathbf{s},\mathbf{s}'}(X)\Big)
\end{aligned}$$

where the polynomials $G^1_{\mathbf{s},\mathbf{s}'}(X)$ and $G^2_{\mathbf{s},\mathbf{s}'}(X)$ are given by (24).

Example 7.17. Take the $\mathbb{Q}$-generic polynomial $f^{C_5}_{A,B}(X)$ for C_5 and $M = \mathbb{Q}$. By Proposition 6.1, for $\mathbf{a} = (a,b)$, $\mathbf{a}' = (a',b') \in \mathbb{Z}^2$, if $\mathbf{a}' = (a,\pm b)$ or $\{\mathbf{a},\mathbf{a}'\} = \{(-1,\pm b),(1,\pm b)\}$ then $\mathrm{Spl}_{\mathbb{Q}} f^{C_5}_{a,b}(X) = \mathrm{Spl}_{\mathbb{Q}} f^{C_5}_{a',b'}(X)$. We also see that $f^{C_5}_{a,0}(X) = (X+a)^2(X+a^2-1)(X+1/(a-1))^2$.

For $\mathbf{a} = (a,b)$, $\mathbf{a}' = (a',b') \in \mathbb{Z}^2$ in the range $-50 \le a, a' \le 50$, $1 \le b \le b' \le 50$ with $\mathbf{a} \ne \mathbf{a}'$, $\{\mathbf{a},\mathbf{a}'\} \ne \{(-1,b),(1,b)\}$, we see that the splitting fields of $f^{C_5}_{a,b}(X)$ and of $f^{C_5}_{a',b'}(X)$ over $\mathbb{Q}$ coincide if and only if $(a,b,a',b') \in \bigcup_{i=1}^4 X_i$ where

$$\begin{aligned}
X_1 &= \{(3,3,23,3), (23,3,3,3), (2,2,-28,14)\},\\
X_2 &= \{(16,2,-12,5), (-33,3,-3,3), (-16,13,34,19)\},\\
X_3 &= \{(-3,1,-3,11), (7,3,27,9), (8,11,33,14), (23,5,35,7), (41,11,-15,17)\},\\
X_4 &= \{(-2,1,3,2), (4,1,-6,2), (3,1,13,7), (-2,2,18,4), (31,1,-19,7),\\
&\qquad (-3,3,-33,3), (-2,3,43,6), (12,4,46,10)\}.
\end{aligned}$$

By Theorem 7.13, it can be checked, in the range above and for each of $i = 1,2,3,4$, that $(a,b,a',b') \in X_i$ if and only if the decomposition type of $H^i_{\mathbf{a},\mathbf{a}'}(X)$ over $\mathbb{Q}$ includes 1.

Example 7.18. We take $M = \mathbb{Q}(n)$ and regard n as an independent parameter over $\mathbb{Q}$. We specialize Hashimoto-Tsunogai's generic polynomials $f^{C_5}_{A,B}(X)$ and $h^{C_5}_{A,B}(X)$ by $A := 2n+3$, $B := 1$.

Then we obtain the cyclic quintic polynomial $f^{C_5}_{2n+3,1}(X) = f^{D_5}_{s,t}(X)$ over $\mathbb{Q}(n)$ where $s = n^5+5n^4+12n^3+10n^2-5n-20$, $t = -n^3-5n^2-10n-7$ and

$$h^{C_5}_{2n+3,1}(X) = X^5 - R(n^2+2n+5)X^3 - R^2(X^2+(n+1)X-1)$$

where $R := n^4+5n^3+15n^2+25n+25$. The discriminants of the polynomials $f^{C_5}_{2n+3,1}(X)$ and $h^{C_5}_{2n+3,1}(X)$ with respect to X are given by $R^8(n^3+5n^2+10n+7)^2$ and $R^8(2n^4+7n^3+23n^2+30n+35)^2(n^6+6n^5+19n^4+34n^3+36n^2+10n-5)^2$ respectively.

On the other hand, we take Lehmer's simplest quintic polynomial $g_n(X)$ which is given as

$$\begin{aligned} g_n(X) = X^5 &+ n^2X^4 - (2n^3+6n^2+10n+10)X^3 \\ &+ (n^4+5n^3+11n^2+15n+5)X^2 + (n^3+4n^2+10n+10)X + 1 \end{aligned}$$

(cf. [Leh88]). The discriminant of $g_n(X)$ with respect to X is $R^4(n^3+5n^2+10n+7)^2$. By using the result in [HR], we see that if $s = n^5+5n^4+12n^3+10n^2-5n-20$ and $t = -n^3-5n^2-10n-7$ then the polynomial $g_n(X)$ and Brumer's quintic $f^{D_5}_{s,t}(X)$ has the same splitting field over $\mathbb{Q}(n)$. Hence we conclude that the splitting fields of $f^{C_5}_{2n+3,1}(X)$, of $h^{C_5}_{2n+3,1}(X)$ and of $g_n(X)$ over $\mathbb{Q}(n)$ coincide. By Theorem 7.13, we checked the pairs $(m,m') \in \mathbb{Z}^2$ in the range $-10000 \le m < m' \le 10000$ to confirm that $\mathrm{Spl}_{\mathbb{Q}} g_m(X) = \mathrm{Spl}_{\mathbb{Q}} g_{m'}(X)$ if and only if $(m,m') = (-2,-1)$.

7.5. **The case of the Frobenius group F_{20}.** Let k be an arbitrary field. By the results of the previous subsections, we should treat only the remaining three cases {(I-3),(I-4),(I-5)}.

For the Frobenius group F_{20} of order 20, we take the k-generic polynomial

$$\begin{aligned} f^{F_{20}}_{p,q}(X) = X^5 &+ \Big(\frac{q^2+5pq-25}{p^2+4} - 2p + 2\Big)X^4 \\ &+ \big(p^2-p-3q+5\big)X^3 + (q-3p+8)X^2 + (p-6)X + 1 \ \in\ k(p,q)[X]. \end{aligned}$$

In the case of char $k \neq 2$, as we mentioned in Section 6, we may also take a k-generic polynomial of the Lecacheux's form for F_{20}:

$$\begin{aligned} g^{F_{20}}_{p,r}(X) = X^5 &+ \Big(r^2(p^2+4) - 2p - \frac{17}{4}\Big)X^4 + \Big((p^2+4)(3r+1) + \frac{13p}{2} + 1\Big)X^3 \\ &- \Big(r(p^2+4) + \frac{11p}{2} - 8\Big)X^2 + (p-6)X + 1 \in k(p,q)[X]. \end{aligned}$$

Method 1. Instead of the computation of $\mathcal{R}^1_{\mathbf{s},\mathbf{s}'}(X)$, we construct $F_{20}\times F'_{20}$-relative D''_5-resolvent polynomial $\mathcal{H}_{\mathbf{s},\mathbf{s}'}(X)$ by using the resolvent polynomial $F^1_{\mathbf{s},\mathbf{s}'}(X)$ which is explicitly given in Subsection 7.3. We put

$$\begin{aligned} F^3_{\mathbf{s},\mathbf{s}'}(X) &:= \mathcal{RP}_{\rho'(P),D_5\times D'_5}(X) = F^1_{s,t,\rho'(s'),\rho'(t')}(X) = \rho'\big(F^1_{\mathbf{s},\mathbf{s}'}(X)\big), \\ F^4_{\mathbf{s},\mathbf{s}'}(X) &:= \mathcal{RP}_{\rho\rho'(P),D_5\times D'_5}(X) = F^1_{\rho(s),\rho(t),\rho'(s'),\rho'(t')}(X) = \rho\rho'\big(F^1_{\mathbf{s},\mathbf{s}'}(X)\big). \end{aligned}$$

Then the polynomial

$$\mathcal{H}_{\mathbf{s},\mathbf{s}'}(X) := \prod_{i=1}^{4} F^i_{\mathbf{s},\mathbf{s}'}(X)$$

becomes the formal $F_{20}\times F'_{20}$-relative D''_5-invariant resolvent polynomial $\mathcal{RP}_{P,F_{20}\times F'_{20}}(X)$ by P. Hence we get the following theorem:

Theorem 7.19. *We take the k-generic polynomial $f^{F_{20}}_{p,q}(X)$ (or $g^{F_{20}}_{p,r}(X)$ when char $k \neq 2$). For $\mathbf{a} = (a_1,a_2)$, $\mathbf{a}' = (a'_1,a'_2) \in M^2$, we assume that $G_{\mathbf{a}} \cong G_{\mathbf{a}'} \cong F_{20}$. An answer to the field intersection problem of $f^{F_{20}}_{p,q}(X)$ (or $g^{F_{20}}_{p,r}(X)$) is given by $\mathrm{DT}(\mathcal{H}_{\mathbf{a},\mathbf{a}'})$ as Table 4 shows.*

Table 4

$G_{\mathbf{a}}$	$G_{\mathbf{a}'}$		GAP ID	$G_{\mathbf{a},\mathbf{a}'}$		$\mathrm{DT}(\mathcal{R}^1_{\mathbf{a},\mathbf{a}'})$	$\mathrm{DT}(\mathcal{H}_{\mathbf{a},\mathbf{a}'})$
F_{20}	F_{20}	(I-1)	$[400, 205]$	$F_{20} \times F_{20}$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	20	40
		(I-2)	$[200, 42]$	$(D_5 \times D_5) \rtimes C_2$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 2$	10^2	20^2
		(1-3)	$[100, 11]$	$(C_5 \times C_5) \rtimes C_4$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 4$	5^4	10^4
		(I-4)	$[100, 12]$	$(C_5 \times C_5) \rtimes C_4$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 4$	10^2	10^4
		(I-5)	$[20, 3]$	F_{20}	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5^3, 4, 1$	$10^3, 4^2, 2$

Method 2. We may apply the result of the dihedral case in Subsection 7.3. Indeed, in the case of char $k \neq 2$, we may convert the Brumer's polynomial $f^{D_5}_{s,t}$ to $f^{F_{20}}_{p,q}(X)$ and $g^{F_{20}}_{p,r}(X)$, respectively, by

$$s = \frac{-10 + q\big(p + \sqrt{p^2+4}\big)}{2\sqrt{p^2+4}}, \qquad t = \frac{1}{2}\Big(p + \sqrt{p^2+4}\Big)$$

and

$$s = \frac{-1}{4}\Big(5p + 8r + 2p^2r + (2pr+5)\sqrt{p^2+4}\Big), \quad t = \frac{1}{2}\Big(p + \sqrt{p^2+4}\Big). \tag{25}$$

In general, we need the factoring process of a resolvent polynomial over the biquadratic extension $M(\sqrt{p^2+4}, \sqrt{p'^2+4})$ of M. However, because we should only treat the case $M(\sqrt{p^2+4}) = M(\sqrt{p'^2+4})$, all we need is the factoring algorithm over $M(\sqrt{p^2+4})$. This is also feasible in the case of char $k = 2$ by using the result of Subsection 7.2.

Example 7.20. We take $M = \mathbb{Q}$ and the $\mathbb{Q}$-generic polynomial $g^{F_{20}}_{p,r}(X)$ of the Lecacheux's form for F_{20}. We first see that

$$g^{F_{20}}_{p,2}(X) = \Big(X - \frac{1}{4}\Big)\Big(X^4 + 2(2p^2 - p + 6)X^3 + 2(4p^2 + 3p + 16)X^2 - 4(p-2)X - 4\Big)$$

and the splitting fields of $g^{F_{20}}_{p,2}(X)$ and of $g^{F_{20}}_{-p,2}(X)$ over $k(p)$ coincide. From (25), we also see that $\mathrm{Gal}(g^{F_{20}}_{0,r}(X)/k(r)) \leq D_5$ because the splitting fields of $g^{F_{20}}_{0,r}(X)$ and of $f^{D_5}_{-(4r+5)/2,1}(X)$ over $k(r)$ coincide.

For $\mathbf{p} = (p_1, r_1)$, $\mathbf{p}' = (p_1', r_1') \in \mathbb{Z}^2$ in the range $-100 \leq p_1, p_1' \leq 100$, $-100 \leq r_1 \leq r_1' \leq 100$ with $\mathbf{p} \neq \mathbf{p}'$, $r_1, r_1' \neq 2$, we see that the splitting fields of $g^{F_{20}}_{\mathbf{p}}(X)$ and of $g^{F_{20}}_{\mathbf{p}'}(X)$ over $\mathbb{Q}$ coincide if and only if $(p_1, r_1, p_1', r_1') \in X_1 \cup X_2$ where

$$X_1 = \{(-3,-3,3,0), (1,-8,-1,-1), (11,1,11,7), (-1,10,11,22), (-1,-11,29,0)\},$$
$$X_2 = \{(7,1,-7,4), (11,1,11,13), (11,7,11,13), (11,12,11,62), (11,31,11,73), (-2,6,-2,84)\}.$$

Using Method 2, it can be checked by Theorem 7.13, in the range above and for each of $i = 1, 2$, that $(p_1, r_1, p_1', r_1') \in X_i$ if and only if two quadratic fields $\mathbb{Q}(\sqrt{p_1^2+4})$ and $\mathbb{Q}(\sqrt{p_1'^2+4})$ coincide and the decomposition type of $F^i_{\mathbf{p},\mathbf{p}'}(X)$ over $\mathbb{Q}(\sqrt{p_1^2+4})$ includes 1. We note that $\mathrm{Gal}(g^{F_{20}}_{\mathbf{p}}(X)/\mathbb{Q}) \cong \mathrm{Gal}(g^{F_{20}}_{\mathbf{p}'}(X)/\mathbb{Q}) \cong F_{20}$ for each $(p_1, r_1, p_1', r_1') \in X_1 \cup X_2$.

Acknowledgment. We thank Professor Kazuhiro Yokoyama for drawing our attention to multi-resolvent polynomials and also for his useful suggestions.

References

[Ade01] C. Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, 1761. Springer-Verlag, Berlin, 2001.

[Alb34] A. A. Albert, *On certain imprimitive fields of degree p^2 over P of characteristic p*, Ann. of Math. (2) **35** (1934), 211–219.

[AS26] E. Artin, O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Hamburg Abhandlungen **5** (1926–27), 225–231.

[AV00] P. Aubry, A. Valibouze, *Using Galois ideals for computing relative resolvents*, Algorithmic methods in Galois theory. J. Symbolic Comput. **30** (2000), 635–651.

[Ber76] E. R. Berlekamp, *An analog to the discriminant over fields of characteristic two*, J. Algebra **38** (1976), 315–317.

[BJY86] A. A. Bruen, C. U. Jensen, N. Yui, *Polynomials with Frobenius groups of prime degree as Galois Groups II*, J. Number Theory **24** (1986), 305–359.

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159–179.

[Cha96] R. J. Chapman, *Automorphism polynomials in cyclic cubic extensions*, J. Number Theory **61** (1996), 283–291.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, Heidelberg, 1993.

[Col95] A. Colin, *Formal computation of Galois groups with relative resolvents*, Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), 169–182, Lecture Notes in Comput. Sci., 948, Springer, 1995.

[DeM83] F. R. DeMeyer, *Generic Polynomials*, J. Algebra **84** (1983), 441–448.

[DM03] F. DeMeyer, T. McKenzie, *On generic polynomials*, J. Algebra **261** (2003), 327–333.

[dSL00] B. de Smit, H. W. Lenstra, Jr. *Linearly equivalent actions of solvable groups*, J. Algebra **228** (2000), 270–285.

[GAP] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.10; 2007 (http://www.gap-system.org).

[GK00] K. Geissler, J. Klüners, *Galois group computation for rational polynomials*, Algorithmic methods in Galois theory, J. Symbolic Comput. **30** (2000), 653–674.

[Gir83] K. Girstmair, *On the computation of resolvents and Galois groups*, Manuscripta Math. **43** (1983), 289–307.

[GLV88] M. Giusti, D. Lazard, A. Valibouze, *Algebraic transformations of polynomial equations, symmetric polynomials and elimination*, Symbolic and algebraic computation (Rome, 1988), 309–314, Lecture Notes in Comput. Sci., 358, Springer, Berlin, 1989.

[Has00] K. Hashimoto, *On Brumer's family of RM-curves of genus two*, Tohoku Math. J. **52** (2000), 475–488.

[HH05] K. Hashimoto, A. Hoshi, *Families of cyclic polynomials obtained from geometric generalization of Gaussian period relations*, Math. Comp. **74** (2005), 1519–1530.

[HH05-2] K. Hashimoto, A. Hoshi, *Geometric generalization of Gaussian period relations with application to Noether's problem for meta-cyclic groups*, Tokyo J. Math. **28** (2005), 13–32.

[HHR08] K. Hashimoto, A. Hoshi, Y. Rikuna, *Noether's problem and $\mathbb{Q}$-generic polynomials for the normalizer of the 8-cycle in S_8 and its subgroups*, Math. Comp. **77** (2008), 1153–1183.

[HT03] K. Hashimoto, H. Tsunogai, *Generic Polynomials over* $\mathbf{Q}$ *with two parameters for the transitive groups of degree five*, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003), 142–145.

[HM07] A. Hoshi, K. Miyake, *Tschirnhausen transformation of a cubic generic polynomial and a 2-dimensional involutive Cremona transformation*, Proc. Japan Acad. Ser. A Math. Sci. **83** (2007), 21–26.

[HM] A. Hoshi, K. Miyake, *A geometric framework for the subfield problem of generic polynomials via Tschirnhausen transformation*, to appear in Number Theory and Applications: Proceedings of the International Conferences on Number Theory and Cryptography. Available as preprint: arXiv:0710.0287v2 [math.NT]

[HM-2] A. Hoshi, K. Miyake, *On the field intersection problem of quartic generic polynomials via formal Tschirnhausen transformation*, to appear in Comment. Math. Univ. St. Pauli. Avalilable as preprint: arXiv:0812.4807v2 [math.NT]

[HR] A. Hoshi, Y. Rikuna, *On a transformation from dihedral quintic polynomials into Brumer's form*, in preparation.

[Hup67] B. Huppert, *Endliche Gruppen. I.*, Grundlehren der Mathematischen Wissenschaften 134, Springer-Verlag, Berlin-New York 1967.

[JLY02] C. Jensen, A. Ledet, N. Yui, *Generic polynomials, constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, Cambridge, 2002.

[Kem94] G. Kemper, *Das Noethersche Problem und generische Polynome*, Dissertation, University of Heidelberg, 1994, also available as: IWR Preprint 94-49, Heidelberg.

[KM00] G. Kemper, E. Mattig, *Generic polynomials with few parameters*, Algorithmic methods in Galois theory. J. Symbolic Comput. **30** (2000), 843–857.

[Kem01] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), 139–141.

[Kid05] M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), 427–447.

[Kid06] M. Kida, *Cyclic polynomials arising from Kummer theory of norm algebraic tori*, Algorithmic number theory, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 102–113, 2006.

[KRY] M. Kida, G. Renault, K. Yokoyama, *Quintic polynomials of Hashimoto-Tsunogai, Brumer, and Kummer*, to appear in Int. J. Number Theory.

[KRS] M. Kida, Y. Rikuna, A. Sato, *Classifying Brumer's quintic polynomials by weak Mordell-Weil groups*, preprint. arXiv:0802.0054v1 [math.NT]

[Kih01] O. Kihel, *Groupe des unités pour des extensions diédrales complexes de degré 10 sur* **Q**, J. Théorie Nombres Bordeaux **13** (2001), 469–482.

[Klu02] J. Klüners, *Algorithms for function fields*, Experiment. Math. **11** (2002), 171–181.

[Kom04] T. Komatsu, *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta Math. **114** (2004), 265–279.

[Kom] T. Komatsu, *Generic sextic polynomial related to the subfield problem of a cubic polynomial*, preprint. `http://www.math.kyushu-u.ac.jp/coe/report/pdf/2006-9.pdf`

[Lag1770] J. Lagrange, *Réflexions sur la résolution algébrique des équations*, Mémoires de l'Académie de Berlin (1770), 205-421.

[Lec98] O. Lecacheux, *Constructions de polynômes génériques à groupe de Galois résoluble*, Acta Arith. **86** (1998), 207–216.

[Leh88] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), 535–541.

[LPS03] F. Leprévost, M. Pohst, A. Schöpp, *Familles de polynômes liées aux courbes modulaires $X_1(l)$ unicursales et points rationnels non-triviaux de courbes elliptiques quotient*, Acta Arith. **110** (2003), 401–410.

[MM97] T. Mattman, J. McKay, *Computation of Galois groups over function fields*, Math. Comp. **66** (1997), 823–831.

[Miy99] K. Miyake, *Linear fractional transformations and cyclic polynomials*, Algebraic number theory (Hapcheon/Saga, 1996). Adv. Stud. Contemp. Math. (Pusan) **1** (1999), 137–142.

[Miy03] K. Miyake, *Some families of Mordell curves associated to cubic fields*, J. Comput. Appl. Math. **160** (2003), 217–231.

[Miy04] K. Miyake, *An introduction to elliptic curves and their Diophantine geometry—Mordell curves*, Ann. Sci. Math. Québec **28** (2004), 165–178.

[Miy06] K. Miyake, *Cubic fields and Mordell curves*, Number theory, 175–183, Dev. Math., 15, Springer, New York, 2006.

[Mor94] P. Morton, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory **49** (1994), 183–208.

[Plo87] C. E. van der Ploeg, *Duality in nonnormal quartic fields*, Amer. Math. Monthly **94** (1987), 279–284. Errata: Amer. Math. Monthly **94** (1987), 994.

[RV99] N. Rennert, A. Valibouze, *Calcul de résolvantes avec les modules de Cauchy*, Experiment. Math. **8** (1999), 351–366.

[Ren04] N. Rennert, *A parallel multi-modular algorithm for computing Lagrange resolvents*, J. Symbolic Comput. **37** (2004), 547–556.

[Rik04] Y. Rikuna, *Explicit constructions of generic polynomials for some elementary groups*, Galois theory and modular forms, 173–194, Dev. Math., 11, Kluwer Acad. Publ., Boston, MA, 2004.

[Sch06] A. M. Schöpp, *Fundamental units in a parametric family of not totally real quintic number fields*, J. Théor. Nombres Bordeaux **18** (2006), 693–706.

[SM85] L. Soicher, J. McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), 273–281.

[Sta73] R. P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

[Val95] A. Valibouze, *Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problems*, Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), 456–468, Lecture Notes in Comput. Sci., 948, Springer, 1995.

[Val] A. Valibouze, *Galois theory and reducible polynomials*. Available from `http://www.lix.polytechnique.fr/~max/publications/valibouze/jnt99.dvi`

[Wol03] S. Wolfram, *The Mathematica Book, Fifth Edition*, Wolfram Media, Inc., Cambridge University Press, 2003.

[Yok97] K. Yokoyama, *A modular method for computing the Galois groups of polynomials*, J. Pure Appl. Algebra 117/118 (1997), 617–636.

Akinari HOSHI
Department of Mathematics
Faculty of Science
Rikkyo University
3–34–1 Nishi Ikebukuro Toshima-ku
Tokyo, 171–8501, Japan
E-mail: hoshi@rikkyo.ac.jp

Katsuya MIYAKE
Department of Mathematics
School of Fundamental Science and Engineering
Waseda University
3–4–1 Ohkubo Shinjuku-ku
Tokyo, 169–8555, Japan
E-mail: miyakek@aoni.waseda.jp